

ROBERT E. BUSHNELL*†

HENRY M. ZYKORIE
JOSEPH G. SEEBER°
JOHN C. BROSKY°+*
DARREN R. CREW+*
MATTHEW J. LESTINA†*

MICHAEL D. PARKER
DANIEL A. GESELOWITZ, Ph.D.
(REG. PATENT AGENTS)

† ADMITTED IN MARYLAND
° ADMITTED IN VIRGINIA
+ ADMITTED IN PENNSYLVANIA
‡ ADMITTED IN NEW YORK
* NOT ADMITTED IN D.C.

R. E. BUSHNELL

ATTORNEY AT LAW

1522 K STREET, N.W., SUITE 300
WASHINGTON, D.C. 20005-1202
UNITED STATES OF AMERICA

30 April 1999

INTELLECTUAL PROPERTY LAW

TELEPHONE (202) 638-5740
(202) 408-9040
FACSIMILE (202) 628-0755
FACSIMILE (202) 289-7100
FACSIMILE (202) 628-3835
(410) 747-0022

E-MAIL: BUSHNELL@CWIXMAIL.COM
E-MAIL: REBUSHNELL@AOL.COM

04/30/99

U.S. PTO
1522 K STREET, N.W., SUITE 300
WASHINGTON, D.C. 20005-1202

Assistant Commissioner for Patents
Washington, D.C. 20231

☐ U.S. Postal Service
☐ Via Local Courier
☐ Via International Courier
☐ Via Facsimile No.
☐ Via E-Mail Attachment
☐ Please Acknowledge Receipt
Attorney Docket: P55690

U.S. PTO
1522 K STREET, N.W., SUITE 300
WASHINGTON, D.C. 20005-1202
04/30/99

Submitted herewith is the following patent application:

Inventor: 1) CHANG-HYI LEE
2) HO-SUK CHUNG
3) EN-SEONG KANG

Title: COPY PROTECTION SYSTEM FOR PORTABLE STORAGE
MEDIA

Please find attached hereto an application for patent which includes: Specification and Abstract, Claims, original Declaration And Power of Attorney, Assignment, and a certified copy of the foreign priority document identified below:

Verified Showing of Small Entity Status: **NO**

Drawings: Formal drawings, 9 sheets, Figures 1 through 9

Claim of priority under 35 U.S.C. §119: **YES**

** The Republic Of Korea Application No. 39808/1998 filed on 24 September 1998; and
** The Republic Of Korea Application No. 39809/1998 filed on 24 September 1998.

FEE (see formula below): CHECK IS NOT ENCLOSED

Basic Fee \$380/760 **\$760.00**

Additional Fees:

Total number of claims in excess of 20: ____ times \$9/18 . **\$0.00**

Number of independent claims in excess of 3: 1 times \$39/78 **\$78.00**

Multiple Dependent Claims \$130/260 **\$0.00**

An Assignment is likewise enclosed: Recording Fee \$40 .. **\$0.00**

Filing Non-English specification **\$130.00**

TOTAL FEES FOR THE ABOVE APPLICATION \$968.00

Assistant Commissioner for Patents

30 April 1999

Page Two

Docket No.: P55690

Inventor: 1) CHANG-HYI LEE
 2) HO-SUK CHUNG
 3) EN-SEONG KANG

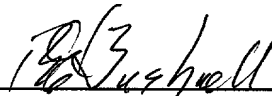
Title: COPY PROTECTION SYSTEM FOR PORTABLE STORAGE
 MEDIA

In view of the above, it is requested that this application be accorded a filing date pursuant to 37 CFR 1.53(b).

Please address all correspondence to:

Robert E. Bushnell
1522 K Street, N.W.
Suite 300
Washington, D.C. 20005

Respectfully submitted,



Robert E. Bushnell
(Registration No. 27,774)
Payor No.: 008-439
Attorney for the Applicant
1522 K Street, N.W.
Suite 300
Washington, D.C. 20005

Telephone: (202) 638-5740
Telefacsimile: (202) 628-0755

REB/kf

TITLE

COPY PROTECTION SYSTEM

FOR PORTABLE STORAGE MEDIA

CLAIM FOR PRIORITY

This application makes reference to, incorporates the same herein, and claims all rights accruing thereto under 35 U.S.C. §119 through our patent applications entitled *The Digital Content Encryption Apparatus And Method Thereof* earlier filed on the 24th day of September 1998 in the Korean Industrial Property Office and there duly assigned Serial Nos. 1998/39808 and 1998/39809.

FIELD OF THE INVENTION

The present invention is generally related to encryption processes and apparatus, and, more particularly, to secure and robust processes and apparatus for the generation and use of keys in the transmission and replay of digital information for licensed SDMI compliant modules such as personal computers and SDMI compliant portable devices in conjunction with Internet service content provider and certificate authority.

BACKGROUND ART

Recently, with the flood of information provided by various media such as broadcasting and press, an atmosphere has been created by the information providers who are interested in providing integrated information that covers all of the media. Other users want to selectively receive a specific

1 item of digital information from the entire spectrum of information available from a particular
2 information provider (IP). Accordingly, a digital content transmission system has been formed by
3 the information providers who convert various types of information into digital form and store this
4 digital information, and the users who subscribe to this digital information system from the
5 information provider via the network. Digital information transmission systems endow an
6 application program with easy downloadability of the digital content. The user can get all the
7 information desired by using this application program to access the digital information system
8 through the network.

9 The digital information may be provided to the user either for pay or for free. In case of paid
10 digital information, the server who provide the digital information via the transmission system sets
11 the service fee. The service server charges the user according to the quantity of information used
12 when the digital information is downloaded to the user. MPEG software protocol for example,
13 compresses audio files to a fraction of their original size, but has little perceptible affect upon the
14 quality of the audio sound. MPEG software protocol is now widely used by Internet sites offering
15 digitalized music, and is reported to be commonly used to offer digitalized versions of recorded
16 music without the consent of the musicians. When a user is connected to a server that provides
17 digital information commercially via a network, a few of the users may be able to inadvertently or
18 illegally copy the digital information, a practice that, as was recently noted by Interdeposit and the
19 French Agency for the Protection of Programs, a member of the European Association of Authors
20 and Information Technology Professional, in the *Patent, Trademark & Copyright Journal*, volume
21 57, No. 1416, page 385 (11 March 1999), would be economically damaging to both the musicians

1 and to the server who is running the digital information transmission system. Currently, the server,
2 as well as the musicians, can do little more than seek redress by undertaking civil and criminal action
3 in an effort to control the possibility of unlicensed reception of digital information. We have noticed
4 that there is a need for a technique to preserve transmission security of revenue bearing information
5 while restricting access to the information by unauthorized entities and preventing unauthorized
6 users from using any of the information that they may be able to illicitly obtain from the information
7 provider by restricting the ability of the unauthorized users to decrypting whatever information they
8 manage to obtain via the system.

SUMMARY OF THE INVENTION

9
10 It is therefore, one object of the present invention to provide improvements in cryptographic
11 processes and apparatus.

12 It is another object to provide a secure and robust digital encryption process and apparatus.

13 It is yet another object to provide digital encryption processes and apparatus endowing a
14 system with secure and robust copy protection for LCM's (*i.e.*, licensed SDMI (*i.e.*, secure digital
15 music initiative) compliant modules such as personal computers) and PD's (*i.e.*, SDMI compliant
16 portable devices such as disk and DVD players) in conjunction with ISP (*i.e.*, Internet service
17 provider) and CA (*i.e.*, certificate authority).

18 It is still another object to provide digital encryption processes and apparatus able to encrypt
19 and transmit digital information received from a transmission system, by the use of multiple
20 cryptographic keys.

1 It is still yet another object to provide digital encryption processes and apparatus for
2 generating and using multiple cryptographic keys during the transmission of digital information to
3 a user.

4 It is a further object to provide digital encryption processes and apparatus that employ user
5 information in the generation and use of multiple cryptographic keys during the transmission of
6 digital information to the user.

7 It is a yet further object to provide digital encryption processes and apparatus able to encrypt
8 and transmit digital information obtained from a transmission system by using multiple
9 cryptographic keys, and to decrypt and play the digital information at the terminal of the user by
10 using a plurality of keys, one of which is common to the multiple keys.

11 It is a still further object to provide digital encryption processes and apparatus able to encrypt
12 and transmit digital information obtained from a transmission system by using key information, a
13 user's key, and a temporary validation key, and to decrypt and play the digital information at the
14 terminal of the user by using the key information and user authorization information.

15 It is still yet a further object to provide encryption, transmission and reception protocols
16 enabling encryption, transmission and decryption of digital information received from a transmission
17 system.

18 It is an additional object to provide encryption, transmission and reception protocols enabling
19 encryption and transmission of digital information received from a transmission system by using
20 multiple keys to encrypt the digital information, and decryption and replay of the digital information
21 at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

1 It is a still yet further object to provide encryption, transmission and reception protocols
2 enabling encryption and transmission of digital information received from a transmission system,
3 by using key information, a user's key, and a temporary validation key, and decryption and replay
4 of the digital information at the terminal of the user by using the key information and user
5 authorization information.

6 It is also an object to provide a more secure cryptograph and process for transmitting
7 information to a terminal of a user who has requested the information.

8 It is also a further object to provide a cryptograph and process that reliably restricts the ability
9 of a registered subscriber who has validly obtained information from an information provider, to
10 deliver that information to another entity in a readily usable form.

11 These and other objects may be attained with an encryption process and apparatus that
12 provides a secure and robust copy protection system for a licensed secure digital music initiative
13 compliant modules such as personal computers and portable devices, in conjunction with Internet
14 service providers and certificate authorities, by responding to a user's request for transmission of
15 items of digital information to the user's terminal unit, by providing copy protection during
16 downloading and during uploading of the digital contents. In order to prevent the digital contents
17 from being copied illegally, a plurality of keys are generated and held by both the user and the digital
18 content provider, and a secret channel is formed between both the user and the digital content
19 provider. The header of the encrypted digital content is encrypted by using a physical address of a
20 sector of a licensed SDMI compliant module such as a portable computer or a portable media device
21 in order to prevent the digital content from being copied illegally after the digital content is recorded

1 in the portable media.

2 BRIEF DESCRIPTION OF THE DRAWINGS

3 A more complete appreciation of this invention, and many of the attendant advantages
4 thereof, will be readily apparent as the same becomes better understood by reference to the following
5 detailed description when considered in conjunction with the accompanying drawings in which like
6 reference symbols indicate the same or similar components, wherein:

7 Fig. 1 is a block diagram illustrating the overall architecture of an implementation of the
8 principles of the present invention;

9 Fig. 2 is a block diagram illustrating a registration by an original equipment manufacture of
10 a portable device with a certificate authority;

11 Fig. 3 is a block diagram showing the registration of a Internet service provider's registration
12 with a certificate authority;

13 Fig. 4 is a block diagram showing the registration of a personal computer and a portable
14 device with an Internet service provider;

15 Fig. 5 is a block diagram showing usage rules governing a database of a right management
16 system;

17 Fig. 6 is an exemplified format;

18 Fig. 7 is a block diagram showing the basic architecture for various inputs;

19 Fig. 8 is a block diagram showing control of outsource import; and

20 Fig. 9 is a block diagram showing a copy protection system for portable media.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

1. INTRODUCTION	3
2. OUR OVERALL ARCHITECTURE	3
3. SOME TERMINOLOGIES	4
4. BASIC REQUIREMENTS FOR THE SECURE SETUP OF LCM AND PD	5
4.1. For the LCM	5
4.2. For the PD	5
4.3. For the PM	6
5. INITIALIZATION (KEY SETUP) MECHANISM	6
5.1. Registration of PD manufacturers to CA	6
5.2. Registration of ISP to CA	6
5.3. Registrations of LCM to ISP and of PD to LCM	7
5.4. Registration of Multiple LCMs or Multiple PDs	8
6. COMPONENTS WITHIN LCM AND PD	8
6.1. Functional Components in LCM	8
6.2. Functional Components in PDFM	9
7. SDMI COMPLIANT FILE FORMAT	10
8. SECURE CONTENTS TRANSACTION RULE OVER ISP-LCM-PD-PM	11
8.1. Contents Transaction from ISP to LCM	11
8.2. Contents Transaction from LCM to PD	11
8.3. Contents Transaction from PD to PM	11
8.4. Portability of PM	11
8.5. Transferability of a Content	12
9. OUTSOURCE INPUT	12
9.1. Basic Architecture for a Secure Import Control	12
9.2. Analog Input to PD	14
9.3. Kiosk	14
10. CONCLUSION	14

1. INTRODUCTION

In this manuscript we describe, as Samsung's proposal for the SDMI standardization, the specific roles and processing rules of the LCM (Licensed SDMI Compliant Module, e.g. personal PC) and SDMI Compliant Portable Device (PD).

First, in section 2, we depict our total architecture for a secure Electronic Music Distribution (EMD) as a candidate for the SDMI Compliant EMD. In section 3, for the removal of the ambiguities on some terminologies and for the clear explanation of our proposal, some terminologies are defined. For some basic requirements or basic modules to be preset within LCM or PD for their secure installation and secure content transaction are presented in section 4 and the initialization protocol of LCM and PD is described in section 5. From section 6 to section 8, the secure content transaction protocol over ISP-LCM-PD-PM are described via the appropriate file format appeared in section 7 and using some functional roles facilitated by those in section 6. Furthermore, our proposed SDMI compliant processes for the considerable various outsource inputs to LCM or PD is presented in section 9.

2. OUR OVERALL ARCHITECTURE

In our overall architecture depicted in the following, the ISP (Internet Service(Content) Provider) and PD-Manufacturer should register to CA(Certificate Authority, e.g. SDMI) to achieve their right certificate for SDMI Compliant Role or Product. When an ISP registers to CA, CA issues a certificate to the ISP's Public Key and stores it into its Data Base and hereafter helps a LCM to makes use of this data to authenticate the ISP when it needs to register to the ISP. And when a PD-Manufacturer registers to CA, CA also issues a manufacturer key and its certificate for the manufacturer and stores it into its Data Base and hereafter, by use of this, stipulates a secure PD-Registration to a LCM by checking its certificate validation in the LCM and by constructing a secure channel between them. Note that any ISPs do not have any knowledge about the manufacturers' keys.

While some content transfer between LCM and PD occurs, the right management system may act on the header part of its file format, where, of course, each communication or content transaction among the members appeared in the Fig.2-1 should be done only after their authenticating and constructing a secure channel. As for the right management of contents, our proposal contains Copyright Status, Playback Status, and Transfer Status. In our proposal, the transferability of a content is discriminated from the portability of it. The Kiosk-like machine is to be treated as a LCM, but is to be subject to the groups of copyright holders.

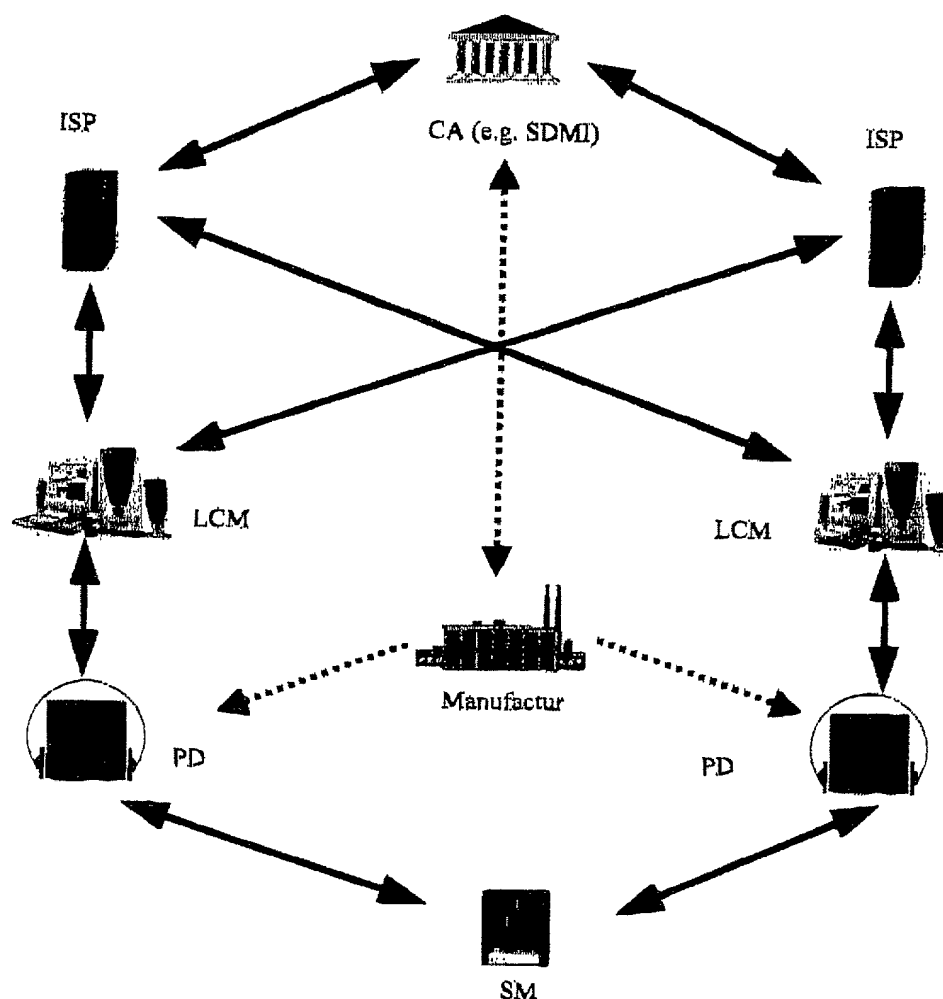


Figure S-1 : The Overall Architecture

3. SOME TERMINOLOGIES

For the removal of some ambiguities, in this section, we define some terminologies and list up some abbreviated words for a simple description (most of them are those commonly used in PDWG). First, we have to distinguish the two words, "Portability" and "Transferability" of a content.

- **Portability** – a content in a PM can be played in *any PD*
- **Transferability** – Portability + "upload of a content is allowed from a PM to even a LCM", in this case the content's uploadability is to be controlled by *check-in/out system* and its *transferability status*.

Hereafter we use the following abbreviated words.

- **CA** – Certificate Authority (e.g. SDMI, or other trust third party)
- **LCM** – Licensed SDMI Compliant Module
- **PD** – SDMI Compliant Portable Device
- **PDFM** – Portable Device Functional Module

- **ISP** – Internet Service Provider (including Content Provider via the Internet)
- **PM** – Portable Media (SDMI Compliant Storage Media)

Furthermore, here are presented some notations to be used in the following sections. Even though they are some intricate, we are sure that they would help the readers clearly understand the concrete method we intend. They are relevant to the algorithmic functional modules.

- **ECC** – Elliptic Curve Cryptosystem
- **PrivKey_A**, **PubKey_A** – Private Key and Public Key of A (this may be LCM, PD (optional), ISP, CA, ...), respectively.
- **Cert_{CA}(PubKey_A)** – A Certificate for a Public Key **PubKey_A** issued by CA.
- **MK_{PD}** – The Manufacturer Key within a PD
- **ID_{MK}** – The Indicator of a Manufacturer Key
- **CK_{PD-LCM}** – This is a secure (secrete) channel key which is setup between PD and LCM
- **EC_ENC(key, C)** – Elliptic Curve Encryption of a content C by utilizing a public key, key. *Where the encryption is the ElGamal-like public key encryption process. And Samsung can support its own ECC implementation technique that is very effective for both S/W and H/W implementation.*
- **EC_DEC(key, C)** – Elliptic Curve based Decryption of a ciphertext (encrypted text) C by utilizing a private key, key.
- **EC_DH(A, B)** – A random secret value (key) shared between A and B by Elliptic Curve based Diffie-Hellman Key Exchanging Protocol.
- **ENC(key, C)** – Symmetric Key Encryption of a content C by utilizing a secrete key, key. *Samsung can support its own Symmetric Key Encryption algorithm, named "SNAKE", that is very effective for both S/W and H/W implementation and it has been world-wide cryptanalized.*
- **DEC(key, C)** – Symmetric Key Decryption of a ciphertext C by utilizing a secrete key, key.

Note: In the above items the Elliptic Curve based Public Key Cryptosystem is just an example as a candidate of Public Key Cryptosystem, and so any public key cryptosystem, for example RSA, can be used instead of it. But we suggest that SDMI Compliant EMD System (Electronic Music Distributing System) adopt the ECC System for the next generation PDs, since ECC can be efficiently implemented in such small devices with low cost.

4. BASIC REQUIREMENTS FOR THE SECURE SETUP OF LCM AND PD

Here we present the minimum substances (algorithms) that are needed for the insurance of the security of LCM and PD. It is assumed that the content compressing and decompressing CODECs are built in each device in either S/W-form or H/W-form.

4.1. For the LCM

- **Public Key Cryptosystem (PKC)** – ECC, RSA, ... (*ECC is more preferable*)
→ This is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the secure channel construction between ISP and LCM.
- **Symmetric Key Encryption Algorithm** – SNAKE, ...
→ This is to be used for the content encryption, the authentication to a PD, and the secure channel construction between LCM and PD.
- **Secure Check-in/Check-out System** – It is to be presented in section 6, 7 how to construct this system and how to securely maintain it.

4.2. For the PD

- **Public Key Cryptosystem (PKC)** – Optional to PD.
- **Symmetric Key Encryption Algorithm** – SNAKE, ...
→ This is to be used for the content encryption, the authentication to a LCM, and the secure channel construction between PD and LCM.
- **Manufacturer Key, MK_{PD}** – the pre-set manufacturer key in a temper resistant area within the PD.

Confidential

Samsung Electronics Co., Ltd.

→ This is to be used for the secure registration of a PD to LCM.

4.3. For the PM

There needs an apparatus or a pre-set special information within a PM to protect contents in it from the dead-copy to another PM. It is desirable, we think, to use the unique ID based approach, that is the method that the manufacturers of PM imbed a unique ID of each PM in the write-protected area of it while they manufacture it. This can be considered as a low cost method to dead-copy protection for the 1st generation PM.

5. INITIALIZATION (KEY SETUP) MECHANISM

There are 4 registration mechanisms relative to ISPs, LCMs, and PDs. The manufacturers' registration to CA is preceded ahead all the others.

5.1. Registration of PD manufacturers to CA

Prior to manufacturing PD, the manufacturers should register to CA to get their manufacturer key, MK_{PD} , and its certificate, $Cert_{CA}(ID_{MK})$, and then produce the SDMI Compliant Portable Devices by using them. Where such registered manufacturer keys are securely stored in CA's DB and only CA maintains the information. The manufacturer should keep their manufacturer-key and its certificate in safe, maintain it securely, and imbed them in a temper resistant area of PDs while he manufactures PDs. In the Fig.5.1-1 an illustrated example is depicted.

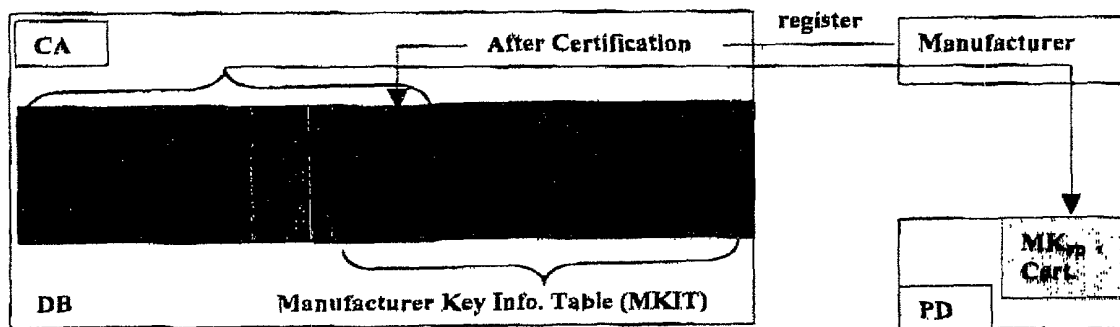


Figure 5.1-1: PD-Manufacturer's Registration to CA

In this figure, when a manufacturer request its registration to CA, CA certifies it and then generates a manufacturer key, MK_{PD} , and make its certificate data, $Cert_{CA}(ID_{MK})$, to deliver them to the manufacturer. At the same time CA generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for the other ISP-registration. Once after a manufacturer got the data, $\{MK_{PD}, Cert_{CA}(ID_{MK})\}$, he/she can manufactures PDs by imbedding those secrete data within a temper resistant area of PDs.

5.2. Registration of ISP to CA

The following Fig.5.2-1 shows how for an ISP to register to CA and what information to get from CA. For an ISP to register to CA, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between CA and itself by $EC_DH(CA, ISP)$. Secondly the ISP gets its semi-permanent private-public key pair $\{PrvKey_{ISP}, PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ and MKIT data appeared in Fig.5.1-1 through the secure channel. Where CA's certification to the ISP should be preceded ahead all these procedures.

Note : ISP's Key Pair should be securely stored.

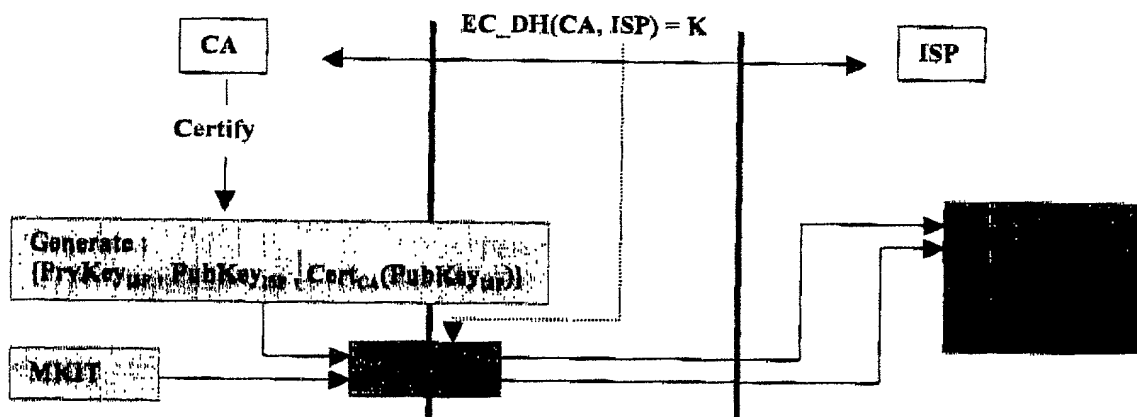


Figure 5.2-1 : ISP Registration to CA

Note : The LCM's Key Pair should be securely stored, where the host's various system parameters may be used for this goal.

5.3. Registrations of LCM to ISP and of PD to LCM

Here the LCM registration mechanism to an ISP together with PD registration is described. As in the Fig.5.3-1 LCM gets the ISP's Public Key Information $\{PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ at first and verifies its validity by using the CA's Public Key Information which was already announced or preset within the LCM in a code-imbedded-like method.

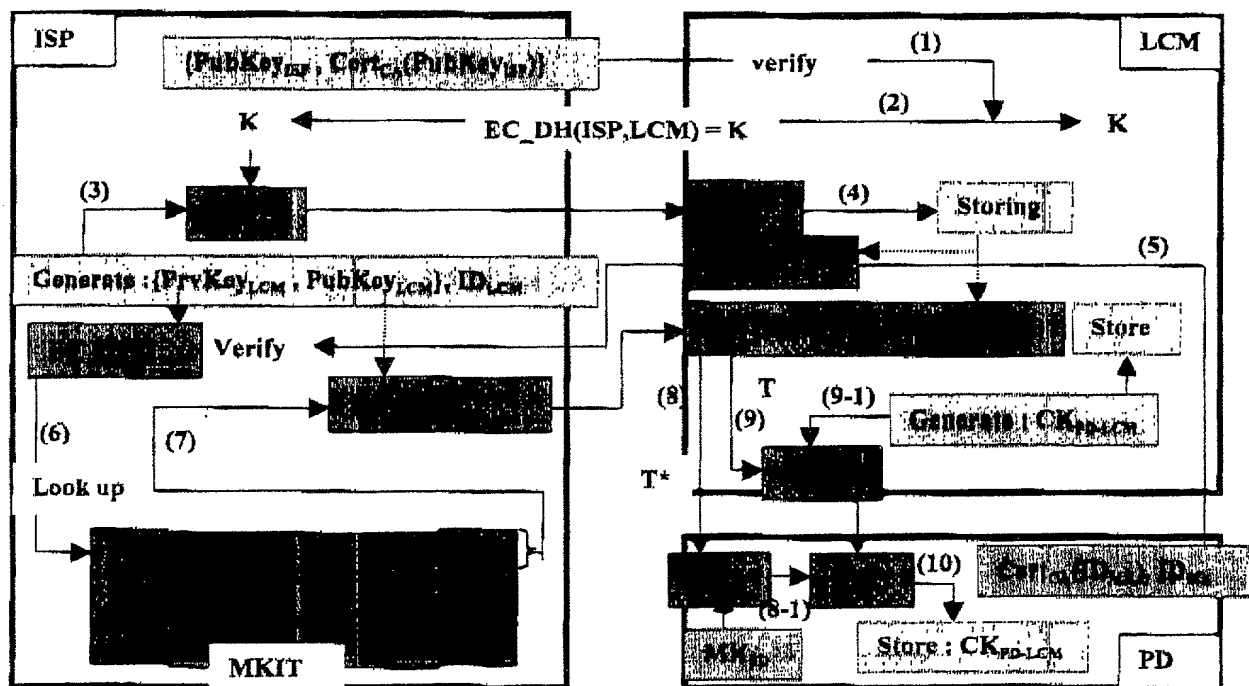


Figure 5.3-1 : LCM and/or PD Registration to ISP

If the validity of the certificate for the ISP's Public Key is certified, the LCM executes the handshaking protocol to get a ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP. For a PD to register to the LCM, it has to toss the certificate data for its ID of manufacturer key and the LCM gets this data from the PD to send this to its connected ISP in the encrypted form, $EC_ENC(PubKey_{ISP}, Cert_{CA}(ID_{MK}))$.

Using this, the ISP can verify the manufacturer key information and can extract its relevant data, $T^*||T$ by looking up MKIP in ISP's DB to transfer it to the LCM in secure manner, i.e. by $EC_ENC(PubKey_{LCM}, T^*||T)$. For the LCM and the PD to setup a shared secret key and to complete the PD registration, the LCM randomly generates their static and secret channel key CK_{PD-LCM} and sends $ENC(T, CK_{PD-LCM})||T^*$. Upon receiving this data, the PD can extract the token value T from T^* and using this token the PD can also compute CK_{PD-LCM} . As the PD securely stores this channel key the PD-registration is finished.

Note1 : The Channel Key CK_{PD-LCM} may be originated from PD instead of LCM. In this case the PD receives the data T^* from the LCM and gets the token T by decrypting T^* with its manufacturer key. And then the PD generates a random channel key CK_{PD-LCM} to upload $ENC(T, CK_{PD-LCM})$ to LCM.

Note2 : The part of the record in MKIT (in LCM) stays in encrypted form by using the LCM's secret key (this key may be LCM's Public Key).

Note3 : In practice, during the PD registration to LCM, the RMS-DB updating token data (UTD, appeared in section 6.1) should be transferred from the PD to LCM(or from the LCM to PD) together with CK_{PD-LCM} and be set both in the RMS-DB and in the PD.

5.4. Registration of Multiple LCMs or Multiple PDs

Our architecture and the file format can allow users to register their own limited number of LCMs or PDs. The number may be limited by ISP or by CA.

- **Registration of Multiple LCMs** → since ISP maintains the private-public key pair of the firstly registered LCM of an user's multiple LCMs, ISP can securely deliver the same key pair to the another LCM of the user's.
- **Registration of Multiple PDs** → since LCM securely maintains the secret channel key between the LCM and PD, the LCM can securely deliver the same key pair to the another PD of the user's in the same manner depicted in Fig. 5.3-1.

6. COMPONENTS WITHIN LCM AND PD

6.1. Functional Components in LCM

• Right Management System

→ To manage the information $CTC=\{\text{Copyright, Transfer, Check-in/Check-out}\}$, LCM has to maintain the Right Management System DB, named RMS-DB in a secure manner. Here we propose our secure Right Management System. In this system we focus on the content transaction between LCM and PD.

The RMS-DB consists of the Title (or Title-ID), CTC field, Playback Control Status (PCS : the permitted times to play, the amnesty period, ...) and Update Token Data (UTD). This DB stays in LCM in the encrypted form by utilizing LCM's secret key. An important characteristic of the Update Token Data (UTD) is that it is generated from PD whenever any content downloading or uploading session between PD and LCM occurs and that it is also stored in the PD.

Whenever a content is played back at first in LCM, the above right management information of the content's file format is newly registered to the RMS-DB. Once a content is registered to the RMS-DB, every playback procedure should priority reference to the DB to check the content's validation. The following Fig.6.1-1 shows exemplified implementation for the management rule of RMS-DB when a content downloading occurs.

Note1 : The part of the record in RMS-DB (in LCM) stays in encrypted form by using the LCM's secrete key (this key may be $CK_{PD,LCM}$).

Note1 : The UTD part may have a few number of Updating Token Data depending on the number of a user's own PDs.

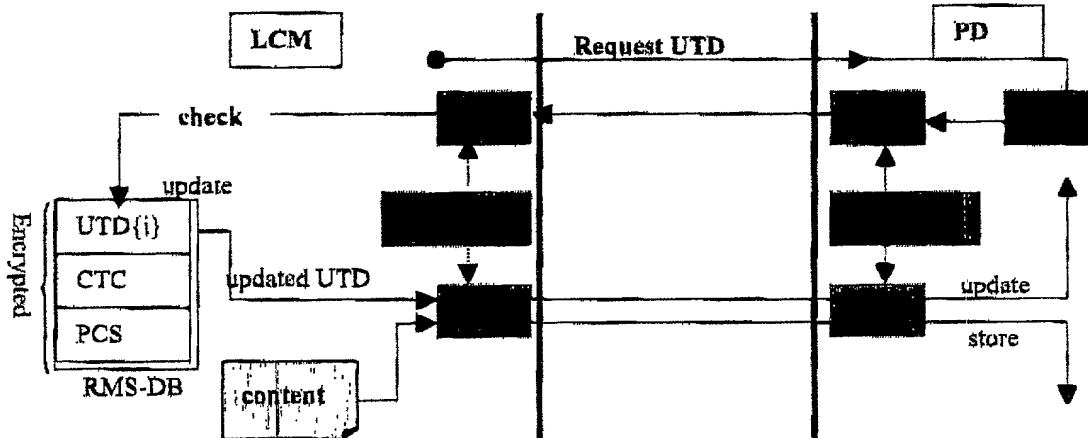


Figure 6.1-1 : Usage Rule of RMS-DB

Note : The RMS-DB may maintain a finite number of UTDs depending on the limited number of users' own PDs which were already registered to the LCM.

- **PD Import Control**

This layer exists in LCM to import SDMI Compliant contents from ISPs or to import non-SDMI Compliant outsource contents (e.g. RedBook CDs, DVD, ...). And so this should contain such capabilities as the followings.

- Trans-Coding → to make PD decompress the input with its CODEC
- Trans-Encrypting → to make PD decrypt the input with its Encryption System
- Converting the input to SDMI Compliant file format

- **PD Interface**

This has the following capabilities.

- Authenticating to PD
- Opening a secure channel between LCM and PD

- **ISP Interface**

This has the following capabilities.

- Authenticating to PD
- Opening a secure channel between LCM and PD

6.2. Functional Components in PDFM

- **LCM Interface**

This has the following capabilities.

- Authenticating to LCM
- Opening a secure channel between PD and LCM

- **Import Control within PDFM**

This has the capability to import a outsource analog input and to make it fit to the SDMI Compliant file format. Where the converted SDMI Compliant content should have the binding information to the PD to be played only via the PD.

7. SDMI COMPLIANT FILE FORMAT

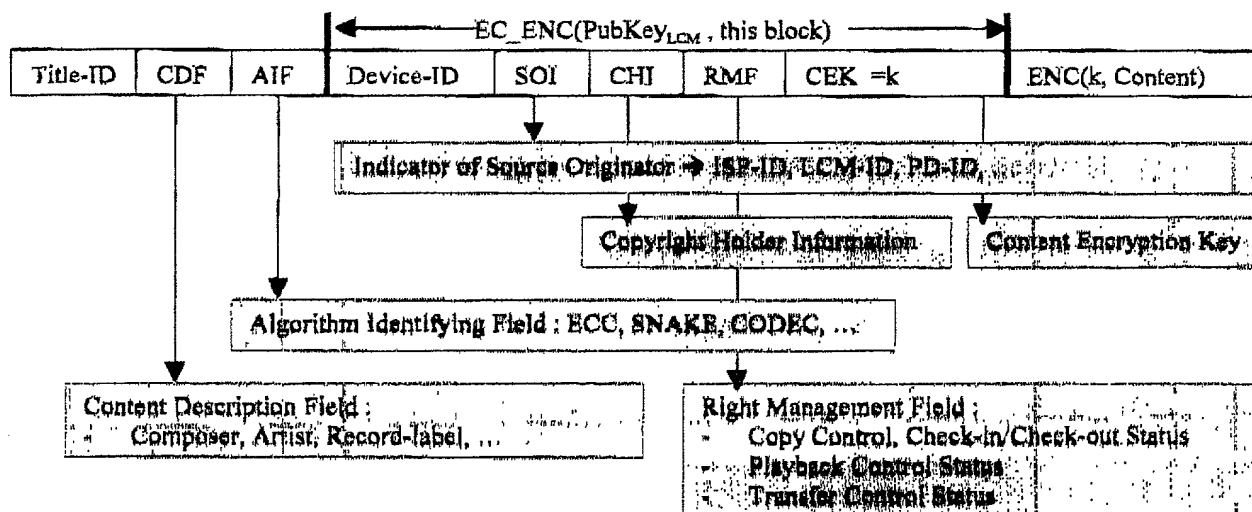
The SDMI-Compliant file format should contain the following information and should allow extendibility and flexibility.

- Indication of Source Originator → ISP, LCM (CD-ripping, Audio input), PD (Analog input), Kiosk, ...
- Device Identifier → LCM_ID, PD_ID, PM_ID
- Algorithm Information Field
 - ✓ Authentication secret sharing algorithm identifier → EC(Elliptic Curve)-Signature, EC-DH, ...
 - ✓ Encryption algorithm identifier → SNAKE, ...
 - ✓ Codec algorithm identifier → MP3, AAC, ...
 - ✓ Encryption key information of content
- Right Management Field

Right management field contains the Copy, Check-In/Out, Transfer and Playback Control Status, which are to be encrypted by secret key of the device.

 - ✓ Copy-Never/Copy-Free/No-More-Copy mode
 - ✓ Check-In/Out mode
 - ✓ Transfer mode (Transferable or not)
 - ✓ Playback Control information
 - Allowable number of times to be played (unlimited or n-times)
 - Expiration date
 - Amnesty period
- Copyright holder information
- Content description field → Title, Composer, Artist, Record-label, ...

Here is illustrated an exemplified file format



We divide the above file format into the following three parts and we call them as in the following.

- Plain-Header (PH) – {Title-ID, CDF, AIF}
- Secret Header (SH) – {Device-ID, SOI, CHI, RMF, Content Encryption Key}
- File Body (FB) – {The Encrypted Content by using the content encryption key in SH}

Confidential

Samsung Electronics Co., Ltd.

8. SECURE CONTENTS TRANSACTION RULE OVER ISP-LCM-PD-PM

8.1. Contents Transaction from ISP to LCM

When an ISP receives a content downloading request from a LCM, it confirms the LCM's ID and then downloads the content with the file format of section 7 to the LCM. For the LCM to play the reached content, it follows the below steps in this order:

- Finding out the encryption algorithm from the field AIF in PH
- Using the found out encryption algorithm and LCM's secret key (private key) to recover the fields in SH
- Comparing the Device-ID field with its ID
- From the RMF information confirming the Copy Control Status, Playback Control Status, and Transfer Control Status to register it to its RMS-DB
- Recovering the content encryption key from CEK to recover the real content from FB
- If any of the above lists does not violate, playing the music.

If it is needed to modify the RMF field, especially the Playback Control Status (PCS), LCM has to replace the data both in the file and in the RMS-DB following the controlling direction.

8.2. Contents Transaction from LCM to PD

The procedure for a LCM to download a content to its PD follows the below steps:

- LCM requests the PD-ID and UTD data to the PD.
- PD sends the $ENC(CK_{PD-LCM}, UTD \parallel PD-ID)$ to the LCM.
- LCM recovers the PD-ID and confirms it.
- LCM recovers the UTD and SH part compares them with those in its RMS-DB.
- If UTD is correct and if any alteration of RMF is needed, the LCM updates the contents of RMF both in RMS-DB and in the file format.
- LCM updates UTD of RMS-DB by newly generated UTD* and $ENC(CK_{PD-LCM}, UTD^*)$ is to be sent to the PD.
- If the Transfer Control Status indicates as "Transfer", then replace it by "Transferred" to the Transfer Control Status field in RMS-DB not in the file format. Where the Transfer Control Status field has the three types, "Transfer", "Transferred", and "Transfer-non".
- If the Copy Control Status (CCS) indicates "Check-in", then replace it by "Check-out" to the Copy Control Status field both in RMS-DB and in the file format.
- If the Copy Control Status (CCS) indicates "Copy-Never", the content downloading to a PD is denied.
- If any of the above lists does not violate, download the content to the PD.

8.3. Contents Transaction from PD to PM

- For the case that a unique ID of each PM exists :
For a PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using the unique ID of the PM as an encryption key.
- For the case that a unique ID of each PM does not exist :
For a PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using a randomly generated key. Where the randomly generated key, say T, is encrypted by a common secret key, S (this is a preset value by the manufacturer of the PD), and is also written on a hidden area of the PM.

8.4. Portability of PM

Confidential!

Samsung Electronics Co., Ltd.

For the first case of the section 8.3, all contents within the PM can be played by all PDs, but, for the second case, all contents within the PM can be played only by the PDs produced by the manufacturers which adopted this system. Any way it is certain that this system can supports the portability of contents via PMs.

8.5. Transferability of a Content

As previously we defined in section 3, the "Transferability" is a different concept from the "Portability" of a content. The main difference is that the content with "Transferability" can be not only played in any PDs but also uploaded to any LCMs, but not in the case of "Portability". Since our system has and manages the Transfer Control Status field both in the RMS-DB and in the file format, our system can support the transferability of a content. If there is marked "Transfer" in the field of a content and if the content is just downloaded to PD, then the LCM downloads it to the PD and replaces "Transfer" by "Transferred" in the relevant field of RMS-DB. Then the content, which has been downloaded to a PD, can no longer be played in the LCM until it is uploaded to the LCM again, but the downloaded content in a PM can be played by any PDs and can be uploaded to another LCM via a PD.

Note : If the Copy Control Status (CCS) of a content contained in a PM indicates "Copy-Free", the content can be uploaded to any LCMs.

9. OUTSOURCE INPUT

As shown in the Fig.9-1, various inputs such as originated from RedBook CD, Audio CD, Super Audio CD, DVD Disk, and analog Device are all allowable to LCM optionally. An analog input to PD is also allowable. The secure import control for those several inputs to LCM or to PD is presented in the next subsections.

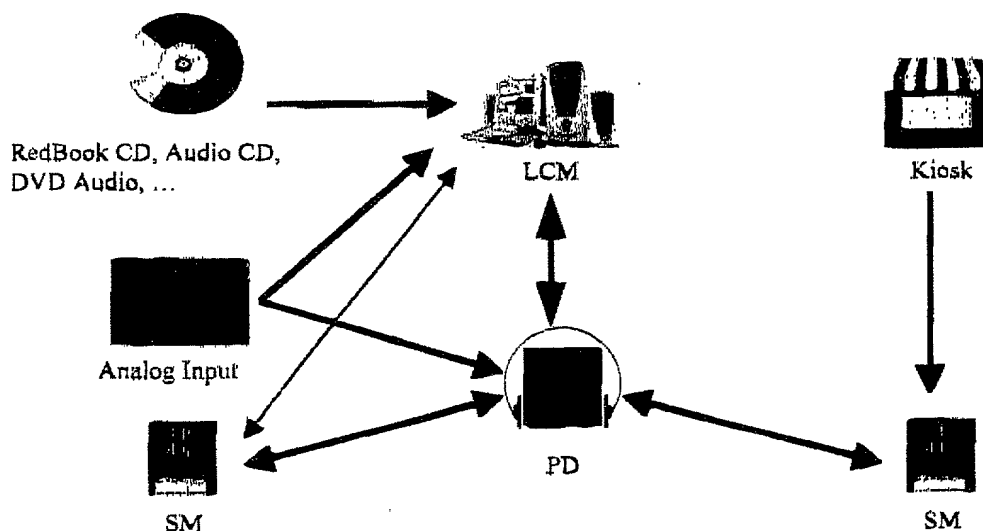


Figure 9-1 : Outsourced Input to LCM and PD

9.1. Basic Architecture for a Secure Import Control

As shown in the Fig.9.1-1, the host device, in which the LCM module exists, has at least the following three layers (two of these exist in the LCM module).

Confidential

Samsung Electronics Co., Ltd.

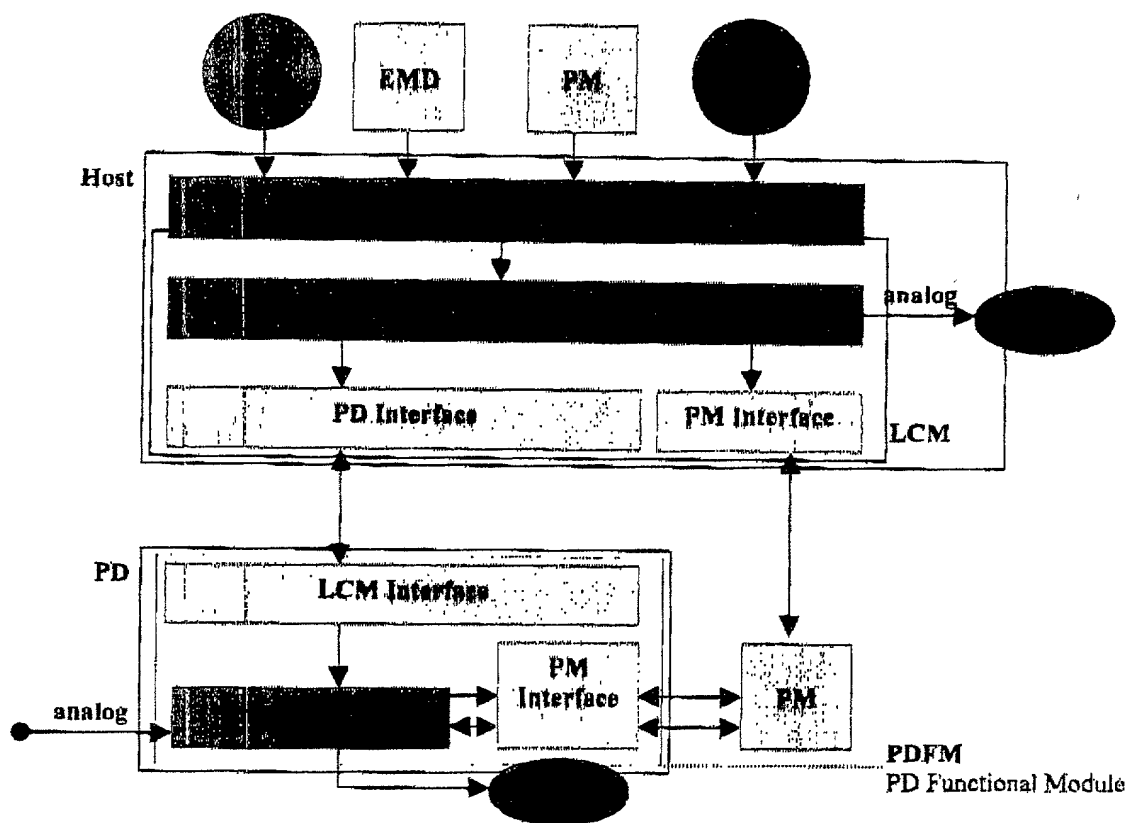


Figure 9.1-1 : Outsource Import Control

- **Authenticated Input API**

This API has the roles that confirms the validity of the input and extracts some required information to convert the input into a SDMI Compliant format.

- **Validity Check**
 - If the input data has a watermark, then this API should be able to detect it.
 - If the input data takes an encrypted (or scrambled) form, then this API should be able to extract its encryption key and the encryption (or scrambling) algorithm.
 - If the input data does not take any protected form, then the API should confirm the validity of written format of the media containing the input data.
- **Required data for the API to pass over to the Import Control Layer.**
 - Information of the media (source) type → Audio CD, DVD Audio, ...
 - Information of the originator of the input content
 - Information of the content → Title, if any, Player, Artist, ...
 - Information of the encryption algorithm if any
 - Information of the encryption key if any

- **PD Import Control**

This Import Control Layer gets a bundle of information from the Authenticated Input API and reconstructs the input content to meet a SDMI Compliant file format by following the rules listed below:

- Copy Control Status → mark "Copy-Never" or "Check-in/Check-out" (optionally)
- Playback Control Status → mark "Times to playback = infinite or N" (N: optional)
- Transfer Control Status → mark "Transfer-Non"
- Mark the "LCM-ID" into the SOI field and Device-ID field of SH(Secret Header)
- If the input content is not encrypted, then generate a random key and encrypt it by the key.
- If the input content takes an encrypted form by other encryption algorithm different from the PD's, then this layer trans-encrypts the content to be played in the PD.
- Public-Key-Encrypt such made secret header part by LCM's public key.

● PD Interface

This layer authenticates the connected PD by checking whether the PD has its correct ID and the secret channel key, $CK_{PD/LCM}$. Where the Kerberos Authentication Protocol may be used (refer to : A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, pp.401-403, CRC Press, 1996).

9.2. Analog Input to PD

The Import Control Layer (ICL) within the PDFM makes a SDMI Compliant compressed digital content from the analog input by following the rules listed below:

- Upon reception of each frame of the analog input, the ICL does encoding the frame and does encrypting it by a randomly generated key. If all the frames has been encrypted follow the next steps.
- Copy Control Status → mark "Copy-Never" or "Check-in/Check-out" (optionally)
- Playback Control Status → mark "Times to playback = infinite or N" (N: optional)
- Transfer Control Status → mark "Transfer-Non"
- Mark the "PD-ID" into the SOI field and Device-ID field of SH(Secret Header)
- Encrypt such made secret header part by PD's channel key.

Note : If such converted SDMI Compliant content from the analog input has its SOI field of SH(Secret Header) with marked "PD-ID", then the procedure of writing the content on a PM does not use the unique ID of the PM. → This means that such content as made from an analog input to a PD is not allowed to have the "Portability".

9.3. Kiosk

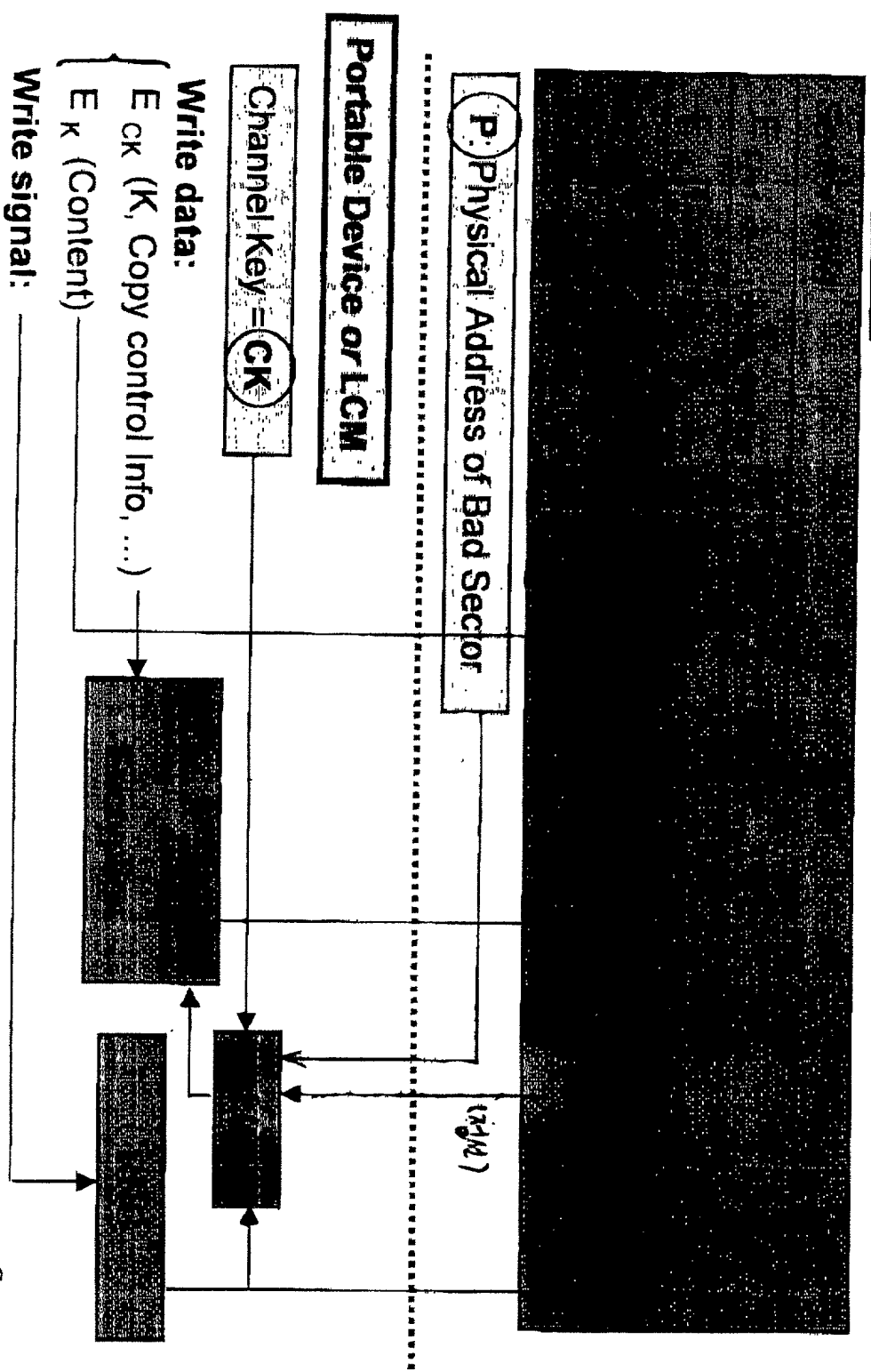
An example for the "Kiosk" may be a shop or a machine that makes a bundle of SDMI Compliant contents into PMs from CD-Ripping, etc. and sells them. Here we regard such Kiosk-like machine as a special LCM with PM-Interface that has a special contraction with some ISPs and groups of copyright holders. Hence, to make a SDMI Compliant PMs from other physical media, the Kiosk-like machine follows the same routines as described in section 9.1 and 9.3.

10. CONCLUSION

In this article we proposed a secure copy protection mechanism for the Internet based MOD Services. One of our proprietary modules is relevant to the use of and management of MKIT table appeared in the PD registration procedure. Another one is relevant to the construction of secure Check-in/Check-out System which securely maintains the contents downloading /uploading between LCM and PD.

SAMSUNG Copy Protection Scheme for Portable Media

SmartMedia



00000000 00000000

Samsung Electronics

SAMSUNG Copy Protection Scheme for Portable Media

1. Unique ID, ID (Optional feature)

- PM may *optionally* support unique ID for 1st Generation PM.
- If Unique ID is not supported, Physical address of bad sector of PM is used instead.
- If unique ID is supported, it should be one-time writeable during manufacturing stage only, and readable only by PD with a special command.

2. Channel Key, CK

- CK is a shared key between LCM and PD.
- To support portability, CK is not considered as input to function f().
- If CK is included, it provides additional security to the content stored in PM.
- CK may take various forms depending on the application usage and right management rules.

3. Physical Address of Bad Sector of Portable Media, P

- The usage of P prevents the playback of illegally copied content from PM to PM by simple "dead-copy"

4. Spared Area

- A special command known only to the manufacturer needs to be known to access this area.

【명세서】

【발명의 명칭】

디지털 콘텐츠 무단 복제 방지 시스템(System for protecting copy of digital contents)

【도면의 간단한 설명】

도 1은 본 발명인 디지털 콘텐츠 무단 복제 방지 시스템을 설명하기 위한 개략적인 도면.

도 2에서 도 5은 도 1에 적용된 각 블록들이 등록요청 또는 디지털 콘텐츠를 재생시키고자 하는 경우에 대해 간단히 설명하기 위한 도면이고,

도 6은 본 발명이 지원하는 파일 포맷의 일 예를 도시한 도면,

도 7은 본 발명에 부가적으로 연결될 수 있는 출력소오스를 도시한 도면,

도 8는 도 7의 출력소오스를 지원하기 위한 입력 제어 블록도를 도시한 도면이다.

도면의 주요부분에 대한 부호설명

10 : 권한부여수단

20 : 휴대 단말기 공급수단

30 : 콘텐츠 공급수단

40 : PC

50 : 휴대용 단말기

60 : 저장매체

【발명이 속하는 기술분야 및 그 분야의 종래기술】

보다 상세하게는 사용자가 재생하고자 다운받은 암호화된 디지털 콘텐츠가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크리트 채널을 이용하여 디지털 콘텐츠를 다운로드 또는 업로드하는 디지털 콘텐츠 무단 복제 방지 시스템에 관한 것이다.

그러므로 상술한 PC에 좀더 많은 디지털 정보를 제공하고자 하는 디지털 콘텐츠 공급자들이 존재하게 되었다. 상술한 디지털 콘텐츠는 단순한 문서 정보뿐만 아니라 MP3와 같은 오디오 파일도 있다.

그러나, 상술한 바와 같이 종래 기술에서는 사용자에게 한번 제공된 디지털 콘텐츠가 무단 복제되는 경우 디지털 콘텐츠 공급자가 이를 방지하기 어렵다는 문제점이 있었다.

본 발명은 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템에 관한 것이다.

보다 상세하게는 휴대용 저장매체 제조시 발생하는 불량색터의 물리적 주소를 이용하여 휴대용 저장매체에 저장되는 암호화된 디지털 콘텐츠의 헤더를 다시 암호화시켜 휴대용 단말기를 통해 다운로드받은 디지털 콘텐츠를 저장매체를 통해 불법으로 복제할 수 없도록 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템에 관한 것이다.

최근 통신환경이 급속도로 발전하고, 각 개인이 통신장비가 구비된 PC를 가지고 있으며, 이 PCLCM을 여러 가지 정보를 접할 수 있게 되었다. *sw, game, v/w → internet appliance (pc, phone, pda, web phone, multi-function mobile phone)*

그러므로 상술한 PCLCM에 좀더 많은 디지털 정보를 제공하고자 하는 디지털 콘텐츠 공급자들이 존재하게 되었다. 상술한 디지털 콘텐츠는 ~~단순한 문서 정보뿐만 아니라 MP3와 같은 오디오 파일도 있다~~ Audio/Video 정보뿐만 아니라 음악가사, 영화자막 등의 문자정보도 있다..

상술한 디지털 콘텐츠는 PCLCM뿐만 아니라 ~~MP3 (MP3로 국한 시키지 않겠)~~ MP3 말고도 AAC, G2 등 ~~많은~~ *저희 제안은 여러종류의 Codec을 지원함* 플래이어인 휴대용 단말기에 다운로드받아 재생시킬 수 있다. 그리고 휴대용 저장매체를 통해 다운로드받아 다른 휴대용 단말기에 장착시켜 재생시킬 수 있다.

이때, 휴대용 저장매체는 ~~스마트 미디어 (스마트미디어로 국한 시키지 않겠)~~ 매체로서, 데드 카피를 하게 되는 경우, 디지털 콘텐츠가 불법으로 복제된다는 문제점이 있었다.

【발명이 이루고자하는 기술적 과제】

따라서, 본 발명의 목적은 전술한 문제점을 해결할 수 있도록 사용자가 재생하고자 다운받은 암호화된 디지털 콘텐츠가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크릿 채널을 이용하여 디지털 콘텐츠를 다운로드 또는 업로드하는 디지털 콘텐츠 무단 복제 방지 시스템을 제공함에 있다.

따라서, 본 발명의 목적은 전술한 문제점을 해결할 수 있도록 휴대용 저장매체 제조시 발생하는 블랑섹터의 물리적 주소를 이용하여 휴대용 저장매체에 저장되는 암호화된 디지털 콘텐츠의 헤더를 다시 암호화시켜 휴대용 단말기를 통해 다운로드받은 디지털 콘텐츠를 저장매체를 통해 불법으로 복제할 수 없도록 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템을 제공함에 있다.

【발명의 구성 및 작용】

이와 같은 목적을 달성하기 위한 본 발명은, 암호화된 디지털 콘텐츠를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키 및 제조키 정보를 생성, 송출하고, 디지털 콘텐츠를 제공할 수 있는 인증 자격 키 및 그 키정보를 암호화하여 송출하는 권한부여수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 콘텐츠를 제공할 수 있는 자격을 부여하기 위해 권한부여수단에서 생성된 한쌍의 키와 그 키정보를 전송받는 콘텐츠 공급수단과, 콘텐츠 공급수단에서 공급하는 디지털 콘텐츠를 공급받아 재생, 출력시키고자 등록 요청신호를 콘텐츠 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보 및 디지털 콘텐츠를 공급받을 수 있도록 암호화된 한쌍의 키와 그 키정보를 전송받는 PC를 포함한다.

또한, 상술한 목적을 달성하기 위한 본 발명은, 암호화된 디지털 콘텐츠를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기

제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 콘텐츠를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키정보를 생성하여 송출하는 권한부여수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단과, 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 콘텐츠를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상기 권한부여수단의 제 2 테이블을 전송받는 콘텐츠 공급수단과, 콘텐츠 공급수단에서 공급하는 디지털 콘텐츠를 공급받아 재생, 출력시키고자 등록 요청신호를 콘텐츠 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 Public Key와 Public Key 정보를 전송받고, 제조키 정보를 콘텐츠 공급수단을 바이패스시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보를 검출하여 암호화한 후 전송하는 PC와, 권한부여수단에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC를 통해 콘텐츠 공급수단으로 제조키 정보를 송출하며, 상기 PC에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의 제조키 정보를 입력받는 휴대용 단말기를 포함한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시 예를 상세히 기술하기로 한다.

도 1은 본 발명인 디지털 콘텐츠 무단 복제 방지 시스템을 설명하기 위한 개략적인 도면으로서, 도시된 바와 같이 그 구성은 다음과 같다.

권한부여수단(10)은 암호화된 디지털 콘텐츠를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기 제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 콘텐츠를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키 정보를 생성하여 송출한다.

휴대용 단말기 공급수단(20)은 상술한 권한부여수단(10)으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는다.

콘텐츠 공급부(30)는 상술한 권한부여수단(10)으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 콘텐츠를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상술한 권한부여수단(10)의 제 2 테이블을 전송받는다.

PC(40)는 콘텐츠 공급수단(30)에서 공급하는 디지털 콘텐츠를 공급받아 재생, 출력시키고자 등록 요청신호를 콘텐츠 공급수단(30)으로 송출하고, 상기 등록 요청신호에 의해 발생된 Public Key와 Public Key 정보를 전송받고, 휴대용 단말기(50)의 제조키 정보를 콘텐츠 공급수단(30)으로 바이패스시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보만 검출하여 암호화한 후 전송한다.

휴대용 단말기(50)는 상기 권한부여수단(10)에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC(40)를 통해 콘텐츠 공급수단(30)으로 제조키 정보를 송출하며, 상술한 PC(40)에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의

제조키 정보를 입력받아 저장한다.

이와 같이 구성된 본 발명에 따른 디지털 콘텐츠 무단 복제 방지시스템의 동작을 첨부한 도면을 참조하여 좀 더 구체적으로 설명한다.

도 2에서 도 5는 도 1에 적용된 각 블록들이 등록요청 또는 디지털 콘텐츠를 재생시키고자 하는 경우 이에 대한 키, 키정보 흐름을 설명하기 위한 도면이다.

도시된 바와 같이, 먼저 휴대용 단말기 공급수단(20)은 권한 부여 수단(10)에 제조한 휴대용 단말기(50)를 등록시키기 위한 등록 요청신호를 송출한다.

그러면, 권한부여수단(10)은 각 휴대용 단말기(50)가 고유하게 가질 수 있는 제조 키(MK_{pd}) 및 제조 키 정보($Cert_{CA}(MK_{pd})$)를 생성하여 휴대용 단말기 공급수단(20)으로 전송한다.

그러므로 휴대용 단말기 공급수단(20)은 휴대용 단말기(50)를 제조하는 과정에서 권한부여수단(10)으로부터 부여받은 제조 키 및 그 제조 키 정보를 휴대용 단말기(50)의 템퍼리 레지스터 영역(temperary resistant area)에 다른 사용자가 알 수 없도록 저장시켜 놓는다.

한편, 권한부여수단(10)은 상술한 바와 같이 휴대용 단말기 공급수단(20)에 제공할 제조 키 및 제조키 정보를 생성함과 동시에 랜덤하게 트콘을 생성한다.

즉, 권한부여수단(10)은 두 개의 테이블을 가지고 있는데, 제 1 테이블은 권한부여수단(10)이 가지고 있는 테이블로서, 상술한 제조 키 및 제조 키 정보를 갖는 테이블이다.

한편, 제 2 테이블은 권한부여수단(10)이 콘텐츠 공급수단(30)에게 전송해

주는 제조 키 정보 테이블(Manufacture Key Information Table)로서, 휴대용 단말기(50)의 ID(Identifier; 식별자), 제조 키에 의해 암호화된 토큰, 토큰에 대한 정보를 갖는 테이블이다.(첨부 도면 도 3참조)

이렇게 해서 상술한 휴대용 단말기 공급수단(20)에서 공급되는 휴대용 단말기(50)는 권한부여수단(10)에 암호화된 디지털 콘텐츠를 다운로드받아 재생시킬 수 있는 권한을 부여 받은 것이다.

또한, 콘텐츠 공급수단(30)도 휴대용 단말기 공급수단(20)과 마찬가지로 권한부여수단(10)으로부터 권한을 부여받아야 하는데, 그러기 위해서 콘텐츠 공급수단(30)은 권한부여수단(10)에게 등록 요청 신호를 송출한다.

그러면 권한부여수단(10)와 콘텐츠 공급수단(30) 사이에는 첨부 도면 도 2와 같이 키 및 키 정보가 생성된다.

즉, 콘텐츠 공급수단(30)으로부터 등록요청신호를 입력받으면 권한부여수단(10)은 자신이 가지고 있는 Private Key 및 Public Key인 $PrvKey_{eph}$, $PubKey_{eph}$ 가 생성된다.

그리고, 콘텐츠 공급수단(20)에 반영구적으로 남게 되는 상술한 바와 같이 한쌍의 키와 그 키정보인 $\{PrvKey_{isp}, PubKey_{isp}, Cert_{CA}(PubKey_{isp})\}$ 가 생성되고, 제조 키에 따라 두 개의 테이블이 생성된다.

그리고, 상술한 권한부여수단(10)과 콘텐츠 공급수단(20)은 EC_DH(CA, ISP)로 생성되는 키를 채널 키로서 상호간에 공유하고, 공유한 채널 키에 의해 상호간에 채널이 안전하게 형성되므로 불법적인 사용자가 상술한 채널로부터 어떠한 정보도

다운로드할 수 없다.

한편, 권한부여수단(10)은 상술한 채널을 통해 생성시킨 키와 키정보를 공유 키로 암호화한 후 콘텐츠 공급수단(50)으로 전송한다. 그러면 권한부여수단(10)과 함께 공유하고 있는 키를 이용하여 전송된 정보를 해독시킨 후 콘텐츠 공급수단(50)에 구비된 저장수단에 저장시킴으로써, 권한부여수단(10)과 콘텐츠 공급수단(30) 사이의 셋업은 종료된다.

상술한 과정이 수행된 후 PC(40)가 콘텐츠 공급수단(30)으로부터 암호화된 디지털 콘텐츠를 다운로드받기 위해 등록요청신호를 송출한다. 그러면 콘텐츠 공급수단(30)은 자신의 퍼블릭키와 퍼블릭 키정보인 $PubKey_{ISP}$, $Cert_{CA}(PubKey_{ISP})$ 를 PC(40)로 전송하고, PC(40)는 저장한다.

그리고, EC_DH(ISP, LCM)에 의해 발생된 키는 콘텐츠 공급수단(30)과 PC(40)가 공유하는 채널 키로서, 콘텐츠 공급수단(20)과 PC(40) 사이에 채널을 형성시키고, 이 채널로 안전하게 디지털 콘텐츠를 전송 받을 수 있다.

또한, 콘텐츠 공급수단(30)으로부터 PC(40)의 영구적인 Private Key, Public Key 한쌍이 채널을 통해 안전하게 공급되는데, 이로써 콘텐츠 공급수단(30)과 PC(40)사이에서 안전하게 디지털 콘텐츠를 다운로드 할 수 있는 시스템이 구현된다.

이때, 휴대용 단말기(50)로부터 PC(40)로 등록요청 신호가 입력되면 휴대용 단말기(50)는 권한부여수단(10)으로부터 제공받은 제조 키 정보를 콘텐츠 공급수단(30)의 Public Key를 암호화한 후 PC(40)를 통해 콘텐츠 공급수단(30)으로 전송한

다.

그러면 콘텐츠 공급수단(30)은 전송된 암호화된 정보를 해독하고, 해독된 결과와 제 2 테이블이 가지고 있는 정보와 비교하여 일치하는 정보가 있는 경우 콘텐츠 공급수단(30)은 테이블의 내용을 암호화한 후 PC(40)로 전송하고, PC(40)에서 해독하여 토큰을 얻어낸다.

이때, PC(40)에서 랜덤하게 채널 키(CK_{PD-LCM})가 생성되는데, 이 채널 키는 비밀이 유지될 수 있도록 생성된다. 이때 PC(40)에서 해독된 토큰을 이용하여 상술한 채널 키를 암호화한 후 휴대용 단말기(50)로 전송한다.

그러면, 휴대용 단말기(50)는 저장되어 있는 제조키를 이용하여 전송된 정보 중 콘텐츠 공급수단(30)의 제 2 테이블에서 읽어들이는 정보로부터 토큰 값을 읽어낸다.

그리고, 상술한 바와 같이 읽어낸 토큰 값을 이용하여 암호화된 정보를 해독시켜 채널 키를 얻어내어 저장함으로써, 채널 키를 PC(40)와 공유하게 된다. 이로써, 휴대용 단말기(50)의 등록과정은 끝나게 된다.

이렇게 하여 전체 시스템에서 서로 상호간에 암호화된 디지털 콘텐츠를 전송받을 수 있는 권한을 모두 부여받게 된다.

마지막으로, PC(40)는 콘텐츠 공급수단(30)으로부터 제공받은 디지털 콘텐츠를 휴대용 단말기(50)로 다운로드 해줌에 있어, 무단 복제되는 것을 방지하기 위해 데이터 베이스를 가지고 있다. 이 데이터 베이스는 첨부도면 도 6에 도시된 바와 같이, RMS-DB로 명칭되어 있다.

상술한 데이터 베이스는 PC(40)와 휴대용 단말기(50) 사이에서 이루어지는 디지털 콘텐츠 처리에 적용된다. 여기서, 데이터 베이스를 구성하고 있는 영역을 살펴보면, 먼저 디지털 콘텐츠의 타이틀 또는 타이틀 ID 영역, 업데이트 토큰 정보(UTD) 영역, 디지털 콘텐츠의 현상태에 대한 정보 영역, 재생 제어 정보 영역으로 이루어져 있다.

상술한 데이터 베이스는 PC(40)가 가지고 있는 비밀 키()에 의해 암호화된 형태로 PC(40)에 저장되어 있다. 상술한 내용 중에서 업데이트 토큰의 가장 중요한 특성은 PC(40)와 휴대용 단말기(50) 사이에서 휴대용 단말기(50)에 임의의 디지털 콘텐츠를 다운로드하거나, 또는 휴대용 단말기(50)로부터 PC(40)로 임의의 디지털 콘텐츠를 업로드할 때, 변화가 생기게 된다. 이때 변화된 업데이트 토큰은 휴대용 단말기(50)를 통해 다시 PC(40)로 전송되어 PC(40)에 저장된 업데이트 토큰을 갱신하게 된다.

처음에 PC(40)에서 디지털 콘텐츠를 재생할 때마다 콘텐츠 파일 포맷의 정보가 상술한 데이터 베이스 상에 새롭게 등록된다. 이렇게 데이터 베이스에 등록된 콘텐츠는 매번 재생동작을 수행할 때마다 데이터 베이스를 참조하여 그 합법성을 체크해야 한다.

또한, PC(40)와 휴대용 단말기(50) 사이에서 디지털 콘텐츠를 다운로드하거나, 또는 업로드할 경우 데이터 베이스의 세 번째 영역인 디지털 콘텐츠의 현상태에 대한 정보 영역을 체크함으로써, 디지털 콘텐츠를 상대방에게 복사형식으로 전송된 것인지, 아니면 콘텐츠 자체가 전송되도록 할 것인지를 알 수 있다.

또한 체크 인/아웃을 체크함으로써, 디지털 콘텐츠의 전송상태를 알 수 있다. 즉 체크 인경우는 디지털 콘텐츠가 PC(40)에서 휴대용 단말기(50)로 다운로드되지 않았음을 알려주는 것이고, ~~체크 아웃인~~ 경우는 PC(20)로부터 휴대용 단말기(50)로 디지털 콘텐츠가 다운로드되는 상태이거나, 다운로드된 디지털 콘텐츠가 다시 PC(40)로 업로드된 경우이다.

또한, 맨 마지막 영역은 재생 제어 정보 영역으로서, 재생회수에 대한 정보, 디지털 콘텐츠 재생 만료기간, 디지털 콘텐츠의 사면 기간에 대한 정보로 이루어져 있다.

즉, 상술한 바와 같이 디지털 콘텐츠가 콘텐츠 공급수단(30)으로부터 제공될 때 설정되어 있는 수치로서, 다운로드할 때마다 하나씩 다운카운트시켜 그 재생회수를 제어하는 것이다.

디지털 콘텐츠 재생 만료기간은 재생 회수로 디지털 콘텐츠의 재생, 출력상태를 제어하는 것이 아니라, 다운로드시 이미 설정된 재생 만료기간을 체크하여 그 기간동안만 디지털 콘텐츠를 이용할 수 있도록 한 것으로서, 이 경우 재생 회수는 무관하다.

마지막으로 디지털 콘텐츠의 사면 기간으로서, 콘텐츠 공급수단(30)이 가치가 떨어진 디지털 콘텐츠에 대해서 그 재생회수나, 사용기간을 두지 않은 것으로서, 사용자가 콘텐츠 공급수단(30)으로부터 상술한 디지털 콘텐츠를 다운로드받아 무한정 재생해 청취할 수 있다.

한편, 콘텐츠 공급수단(30)이 PC(40)의 콘텐츠 다운로드 요청을 수락하면,

먼저 PC(40)의 ID를 확인하고 나서, PC(40)로 소정의 파일 포맷을 갖는 콘텐츠를 다운로드한다.

상술한 파일 포맷의 일 예를 첨부 도면 도 6에 의거해서 설명하면 다음과 같다.

본 발명이 지원하는 파일 포맷은 타이틀 ID 필드, 디지털 콘텐츠의 작곡자, 가수, 레코드 라벨과 같은 정보를 갖는 콘텐츠 디스크립션 필드, ECC, SNAKE, CODEC 등과 같은 알고리즘 식별 정보를 갖는 알고리즘 식별필드, 디바이스 ID, ISP_ID, LSP_ID, PD_ID와 같은 현재 정보가 출력되고 있는 소오스출력수단을 표시하는 SOI 필드, 복사 소유자 정보를 나타내는 카피라이트 홀더 인포메이션 (COPYRIGHT HOLER INFORMATION; CHI) 필드, 라이트 매니지먼트 필드, 콘텐츠 암호화 키 필드로 이루어져 있다.

여기서, SOI 필드의 ISP_ID는 본 발명의 콘텐츠 공급수단(30)이며, LSP_ID는 PC(40)이며, PD_ID는 휴대용 단말기(50)이다.

상술한 포맷을 갖는 디지털 콘텐츠를 다운로드 받아 재생하는 경우 PC(40)는 먼저 AIF 필드 또는 PH 필드로부터 암호화 알고리즘을 알아내고, 알아낸 암호화 알고리즘을 이용하여 SH 필드로부터 PC(40)의 Private Key를 복구시킨다.

그리고, PC(40)의 ID와 DEVICE-ID 필드에 있는 ID를 비교하여 일치하는지를 체크하고, RMF 정보로부터 복사 제어 상태, 재생 제어 상태 및 전송 제어 상태를 확인하여 그것을 PC(40)가 가지고 있는 데이터 베이스에 등록시킨다.

그리고 나서, CEK 필드를 이용하여 디지털 콘텐츠 암호화 키를 회복시키고,

실제 디지털 콘텐츠로 복귀시켜 재생할 수 있도록 한다.

PC(40)가 상술한 내용 중 어느 하나라도 위배하지 않을 경우 콘텐츠 공급수단(30)은 PC(40)로 디지털 콘텐츠를 다운로드 시킨다.

만약, RMF필드 중 특히, 재생 제어 상태를 변경할 필요는 경우라면, PC(40)는 데이터 베이스와 파일 포맷에 모두에서 재생 제어 상태 정보를 변경하고자 하는 정보로 대체시켜야 한다.

상술한 바와 같이 PC(40)에서 다운로드한 디지털 콘텐츠를 다시 휴대용 단말기(50)로 다운로드 시켜 재생하고자 하는 경우 다음과 같은 절차를 거쳐야 한다.

먼저, PC(40)에서 휴대용 단말기(50)로 휴대용 단말기 ID와 휴대용 단말기(50)가 가지고 있는 UTD 정보를 요청한다.

그러면 휴대용 단말기(50)는 PC(40)의 채널 키(CK_{PD-LCM})로 UTD를 암호화한 후 휴대용 단말기 ID와 함께 PC(40)로 전송한다. 이때, PC(40)는 휴대용 단말기(50)로부터 전송된 정보를 확인한 후 휴대용 단말기 ID를 복귀시킴과 동시에 데이터 베이스 상에 있는 휴대용 단말기 ID와 비교하여 UTD와 SH 필드를 복귀시킨다.

만약, 상술한 UTD가 정확하나, RMF의 변경이 필요한 경우 PC(40)는 데이터 베이스와 파일 포맷 두군데를 모두 RMF 디지털 콘텐츠로 갱신하여야 한다.

PC(40)는 새롭게 생성된 UTD로 데이터 베이스를 갱신시키고, 새롭게 생성된 UTD는 채널 키(CK_{PD-LCM})에 의해 암호화시킨 후 휴대용 단말기(50)로 전송된다.

만약, 전송 제어 상태는 'Transfer' 상태에서 디지털 콘텐츠가 휴대용 단말기(50)로 전송되고 난 후 'Transferred'로 대체된다. 이때, PC(40)가 갖는 데이터

베이스에는 상술한 전송 제어 상태 필드가 파일 포맷으로 존재하지 않는다. 즉, 전송 제어 상태필드는 'Transfer', 'Transferred', 'Transfer-non'와 같은 세가지 형태를 갖는다.

한편, 복사 제어 상태는 맨처음 체크인(Check-in)으로 지칭되고, 디지털 콘텐츠가 전송되고 난 후 PC(40)가 가지고 있는 데이터 베이스와 파일 포맷 상에서 체크 아웃(Check-out)으로 대체된다.

만약 복사 제어 상태 필드가 '복사 불가(Copy-never)'로 지칭되어 있으면, PC(40)의 디지털 콘텐츠는 휴대용 단말기(50)로 다운로드되지 않는다.

상술한 과정 중 하나라도 위배하지 않을 경우 휴대용 단말기(50)로 디지털 콘텐츠가 다운로드 된다.

시스템에서는 마지막 단계라고 볼 수 있는 휴대용 단말기(50)로부터 저장매체(60)로 디지털 콘텐츠를 처리하는 방법에 대해서 간단히 설명하면 다음과 같다.

첫째, 각 휴대용 저장매체(60)에 고유 ID가 존재하는 경우, 휴대용 단말기(50)에서 저장매체(60) 상에 디지털 콘텐츠를 기록하기 위해, 단지 저장매체(60) 상에 콘텐츠를 기록하고, 기록한 디지털 콘텐츠를 시크리트 헤더(Secret Header)로 복귀하고, 암호화 키로서 저장매체(60) 상에 존재하는 저장매체의 고유 ID를 이용하여 디지털 콘텐츠를 다시 암호화한다.

둘째, 각 저장매체(60)에 고유 ID가 존재하지 않는 경우, 휴대용 단말기(50)에서 저장매체(60) 상에 디지털 콘텐츠를 기록하기 위해, 단지 저장매체(60) 상에 콘텐츠를 기록하고, 기록한 디지털 콘텐츠를 시크리트 헤더(Secret Header)로 복귀

하고, 랜덤하게 발생하는 키를 이용하여 다시 암호화한다.

여기서, 랜덤하게 발생하는 키인 T는 일반적인 시크리트 키인 S에 의해 암호화된다. 이때 일반적인 시크리트 키인 S는 휴대용 단말기의 제조자에 의해 미리 설정되어 있다.

그리고, 상기 암호화된 T는 저장매체(60)의 히든 영역에 기록된다.

상술한 바와 같이 첫 번째 경우, 저장매체(60) 내에 있는 모든 디지털 콘텐츠는 모든 휴대용 단말기(50)에서 재생시킬 수 있다. 그러나, 두 번째 경우 저장매체(60) 내에 있는 모든 콘텐츠는 오직 이 시스템에 채택된 제조자에 의해 생산된 휴대용 단말기에 의해서만 재생시킬 수 있다.

본 발명에서 언급된 디지털 콘텐츠는 임의의 휴대용 단말기 뿐만 아니라 임의의 PC로 업로드시킬 수 있다.

본 발명은 전송 제어 상태 필드를 PC(40)가 갖는 데이터 베이스와 파일 포맷 내에 모두 가지고 있다. 본 발명은 디지털 콘텐츠를 PC(40)에서 휴대용 단말기(50)로 다운로드시킬 뿐만 아니라, 휴대용 단말기(50)에서 PC(40)로 업로드시킬 수 있도록 지원한다.

만약, 디지털 콘텐츠의 필드에 'transfer'이 표시되어 있다면 디지털 콘텐츠를 휴대용 단말기(50)로 다운로드 시키고, PC(40)의 데이터 베이스의 관계되는 필드는 'transfer'에서 'transferred' 표시로 대체되고, 그 변경된 정보를 휴대용 단말기(50)로 다운로드한다.

그리고, 휴대용 단말기(50)에 다운로드된 디지털 콘텐츠는 다시 PC(40)로 업

로드되기 전까지는 PC(40) 상에서 재생시킬 수 없다. 그러나, 저장매체(60)에서 다운로드된 디지털 콘텐츠는 임의의 휴대용 단말기(50)에서 재생시킬 수 있다. 휴대용 단말기(50)를 경우에서 또다른 PC(40)로 업로드시킬 수 있다.

또한, 본 발명이 적용된 PC(40)나, 휴대용 단말기(50)에는 매우 다양한 입력 장치가 부가적으로 연결될 수 있는데, 첨부 도면 도 7에 도시된 바와 같이, PC(40) 및 휴대용 단말기(50)에 부가적으로 연결되는 입력장치로는 RedBook CD, 오디오 CD, 슈퍼 오디오 CD, DVD Disk 및 아날로그 장치 등이 있다.

첨부 도면 도 8은 상술한 도7에 도시된 출력소스(Outsource)의 입력 제어 를 설명하기 위한 도면이다.

도시된 바와 같이, API(응용 프로그램 인터페이스)는 입력이 본 발명이 지원 하는 시스템에 합법적으로 인증된 것인지를 확인하고, 아울러 입력을 본 발명에서 지원하는 파일 포맷으로 전환하기 위해 필요한 정보를 추출하는 역할을 한다.

상술한 입력의 인증 확인은 입력장치의 정보가 수위표를 가질 경우, 상술한 API는 그것을 탐지할 수 있어야 한다. 또한, 입력장치의 정보가 암호화된 형태를 가질 경우 상술한 API는 암호화키와 암호화 알고리즘을 추출할 수 있어야 할 뿐만 아니라 입력장치의 정보가 암호화된 형태를 가질 경우 API는 입력장치의 정보를 포함하는 저장매체에 기록 포맷의 인증 여부를 확인해야 한다.

상술한 API가 입력 제어 층(Import control layer)으로 전달되기 위해 필요한 정보는 저장매체의 종류에 대한 정보, 예를 들면 오디오 CD, DVD 오디오 등이 있다. 또한, 입력되는 디지털 콘텐츠의 초기형태에 대한 정보인 디지털 콘텐츠에

대한 정보, 예를 들면 타이틀, 플레이어, 가수 등이다.

그리고, 암호화 알고리즘에 대한 정보인 암호화 키에 대한 정보는 휴대용 단말기의 입력 제어에서 이 입력 제어 층은 인증된 입력 API로부터 일정량의 정보를 받아서 입력 콘텐츠를 아래에 열거한 규칙에 따라서 본 발명에서 지원하는 파일 포맷에 맞도록 재 구성한다.

복사 제어 상태 즉, '복사불가' 표시, 혹은 '체크 인/체크 아웃(선택적으로)', 재생 제어 상태 즉, '재생회수=무한정 혹은 횟수(선택적)', 전송 제어 상태 즉, '전송불가' 표시, 'LCMLID'를 SOI 필드와 시크리트 헤더의 디바이스 ID 필드로 표시된다.

만약에, 입력되는 디지털 콘텐츠가 암호화되어 있지 않을 경우 랜덤하게 키를 생성하여 그것을 키에 의해 암호화한다. 즉, 입력되는 디지털 콘텐츠가 휴대용 단말기와 다른 종류의 암호화 알고리즘에 의하여 암호화된 형태를 가질 경우 이 층은 휴대용 단말기에 재생되는 콘텐츠를 전환-암호화(Trans-encryption)한다.

그리고, PC가 가지고 있는 Public Key에 의해 시크리트 헤더부분을 Public Key로 암호화한다.

또한, 본 발명에 적용되는 휴대용 단말기의 인터페이스 층은 휴대용 단말기가 정확한 ID와 시크릿 채널 키를 가지는지의 여부를 체크함으로써 연결된 휴대용 단말기를 인증한다.

한편, 상술한 휴대용 단말기로 입력되는 아날로그 입력은 PDFM 내에서의 입력 제어 층은 아래 열거한 규칙에 따라 아날로그 입력으로부터 본 발명에서 지원하

는 압축 디지털 콘텐츠를 만든다.

즉, 아날로그 입력의 각 프레임이 수신되자마자 입력 제어 용은 먼저 그 프레임을 인코딩하고, 랜덤하게 발생된 키를 사용하여 인코딩된 프레임을 암호화한다. 만약 모든 프레임이 암호화되었다면 다음 단계를 따른다.

복사 제어 상태 즉, '복사불가' 표시, 혹은 '체크 인/체크 아웃(선택적으로)', 재생 제어 상태 즉, '재생회수=무한정 혹은 횟수(선택적)', 전송 제어 상태 즉, '전송불가' 표시, PD_ID를 SOI 필드와 시크리트 헤더의 디바이스-ID로 표시한다.

상술한 휴대용 단말기는 자신이 갖는 채널 키에 의해 시크리트 헤더를 암호화한다. 즉, 아날로그 입력으로부터의 전환된 경우 본 발명에서 지원하는 디지털 콘텐츠가 "PD-ID"로 표시된 시크리트 헤더의 SOI 필드를 가질 경우, 저장매체에 디지털 콘텐츠를 기록할 경우 저장매체의 고유 ID를 사용하지 않는다. 이것은 휴대용 단말기로 입력되는 아날로그 입력은 휴대성을 갖지 못한다는 것을 뜻한다.

마지막으로 출력소오스 장치 중 하나인 키오스크는 CD-ripping에서 저장매체로 전송되는 본 발명에서 지원하는 디지털 콘텐츠를 만들어 파는 기계나 상점으로 볼 수 있다.

여기서, 우리는 키오스크류의 기계를 저장매체의 인터페이스를 지닌 특별한 PC로 간주한다. 여기서 저장매체 인터페이스는 저작권 소유자와 디지털 콘텐츠 공급수단만이 특별 계약을 통해 사용할 수 있다.

이와 같은 목적을 달성하기 위한 본 발명에 따른 ~~PGLCM을~~ 통해 디지털

콘텐츠 공급수단으로부터 공급되는 암호화된 디지털 콘텐츠를 입력받아 휴대용 저장
매체로 전송해주는 휴대용 단말기를 갖는 복제 방지 시스템에 있어서(LCM에서 직접
휴대용 저장매체로 저장할 수도 있음), 불량섹터의 물리적 주소, PD (또는 LCM)에
서 발생하여 저장매체의 키영역(Spare Area)에 저장한 랜덤한 수 및 ~~PGLCM~~에서 생
성하여 전송되는 ~~시크릿~~ 키를 ~~채널~~ 입력으로 받아 함수처리하고, 함수 처리된 결과값
으로 디지털 콘텐츠의 헤더를 암호화하여 송출하는 휴대용 단말기와, 상기 휴대용
단말기로 불량섹터의 물리적 주소를 읽어들여 전송하고, 휴대용 단말기에서 랜덤하
게 발생하는 수를 키 값으로 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디
지탈 콘텐츠 및 함수 결과값에 의해 다시 암호화된 헤더 정보를 섹터 데이터로 저
장하는 휴대용 저장매체를 포함한다.

이하, 첨부한 도면들을 참조하여 본 발명의 바람직한 실시 예를 상세히 기술
하기로 한다.

도 1은 본 발명인 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스
템을 도시한 블록도로서, 그 구성은 다음과 같다.

휴대용 단말기(100)는 불량섹터의 물리적 주소, PD (또는 LCM)에서 발생하여 저장매체의 키영역(Spare Area)에 저장한 랜덤한 수 및 PGLCM에서 생성하여 전송되
 는어 휴대용 단말기에 안전하게 저장된 ^{채널} ~~시크릿~~ 키를 입력으로 받아 함수처리하고,
 함수 처리된 결과값으로 디지털 콘텐츠의 헤더를 암호화하여 송출한다.

상술한 휴대용 단말기(100)는 MP3 음악 파일을 다운로드받아 재생시킬 수 있
 는 기기이다.

저장매체(200)는 상기 휴대용 단말기(100)로 불량섹터의 물리적 주소란 ~~의의~~
~~를~~ 전송하고, 휴대용 단말기(100)에서 랜덤하게 발생하는 수를 ~~값~~ f 함수의 입
 력 인자의 일부로써 키영역(Spare Area)으로 저장하며, 휴대용 단말기를 통해 입력
 되는 암호화된 디지털 콘텐츠 및 함수 결과값에 의해 다시 암호화된 헤더 정보를
 섹터 데이터로 저장한다.

상술한 저장매체(200)는 스마트 미디어를 포함한 일반적인 저장매체 이다.

이와 같이 구성된 본 발명에 따른 무단 복제를 방지하기 위한 휴대용 저장매
 체를 갖는 시스템의 동작을 첨부한 도면을 참조하여 좀 더 구체적으로 설명한다.

먼저, 휴대용 단말기(100)는 PGLCM로부터 디지털 콘텐츠를 다운로드 받거나
 직접 콘텐츠 공급수단으로부터 다운로드 받는다.

이때, 휴대용 단말기(100)는 PGLCM으로부터 휴대용 단말기(100)와 PGLCM 사
 이에 안전한 채널을 형성시키기 위해 휴대용 단말기(100) 및 PGLCM는 하나의 시크
 리트 키(~~secret key~~, S-Channel Key, CK)를 공유하게 된다.

그리고, 휴대용 단말기(100)의 입력포트콜 통해 암호화된 디지털 콘텐츠를

입력받아 저장매체(200)로 전송시켜 저장매체(200)의 섹터 데이터 영역에 저장되도록 한다.

그리고 휴대용 단말기(100)는 다운로드 받은 디지털 콘텐츠가 저장매체(200)를 통해 불법 복제되는 것을 방지하기 위해 디지털 콘텐츠의 헤더부분을 다시 한번 암호화시킨다. (원래, 디지털 콘텐츠의 헤더부분은 CK로 암호화되어 LCM에서 휴대용 단말기로 전송된다.) 이때, 암호화 하는 키를 발생시키는 것이 함수처리수단(110)이다.

즉, 상술한 함수처리수단(110)은 저장매체(200)에서 전송하는 불량섹터의 물리적 주소를 입력으로 받는 한편, 휴대용 단말기(100)의 랜덤발생수단(120)을 통해 발생한 랜덤한 수를 입력받는다. 이때 발생된 랜덤한 수는 저장매체(200)의 키영역에도 전송되어 저장된다.

그러므로, 함수처리수단(110)은 상술한 불량섹터의 물리적 주소, 랜덤한 수 및 PCLCM에서 생성한 공유 키를 입력받아 함수 처리하고, 그 결과값을 해독 및 암호 수단(130)으로 입력하여 디지털 콘텐츠의 헤더부분을 다시 암호화시켜 저장매체(200)의 섹터 데이터 영역에 저장시킨다.

이때, 함수처리수단(120)으로 입력되는 불량섹터의 물리적 주소, 랜덤한 수 및 공유 키는 모두 입력받을 수도 있고, 그 중에 하나만 선택적으로 입력받아 함수 처리하여 디지털 콘텐츠의 헤더를 암호화할 수 있다.

【발명의 효과】

따라서, 상술한 바와 같이 본 발명은 전체 시스템이 서로 상호간에 통신을 수행하는 수단끼리 채널 키를 공유하고 안전한 채널을 형성시켜 상호간에 디지털 콘텐츠를 주고 받음으로써, 중간에 불법 사용자가 디지털 콘텐츠를 가져갈 수 없도록 할뿐만 아니라, 합법적인 사용자가 합법적으로 다운로드받은 디지털 콘텐츠라 하더라도 휴대용 단말기도 상술한 구성을 갖고 있기 때문에 상호간에 무단으로 복제되는 것을 방지할 수 있다는 효과를 제공한다.

따라서, 상술한 바와 같이 본 발명은 디지털 콘텐츠가 저장된 저장매체인 ~~스마트 미디어~~를 데드 카피(DEAD COPY)하여 디지털 콘텐츠를 복제하더라도 재생시킬 수 없기 때문에 불법적으로 복제하는 것을 근본적으로 방지할 수 있다는 효과를 제공한다.

What is claimed is:

【청구항 1】

암호화 알고리즘에 의해 암호화된 디지털 콘텐츠를 전송받아 해독한 후 재생, 출력할 수 있는 디지털 콘텐츠 복제 방지 시스템에 있어서,

상기 암호화된 디지털 콘텐츠를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키 및 제조키 정보를 생성, 송출하고, 디지털 콘텐츠를 제공할 수 있는 인증 자격 키 및 그 키정보를 암호화하여 송출하는 권한부여수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 콘텐츠를 제공할 수 있는 자격을 부여하기 위해 권한부여수단에서 생성된 한쌍의 키와 그 키정보를 전송받는 콘텐츠 공급수단; 및

상기 콘텐츠 공급수단에서 공급하는 디지털 콘텐츠를 공급받아 재생, 출력시키고자 등록 요청신호를 콘텐츠 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보 및 디지털 콘텐츠를 공급받을 수 있도록 암호화된 한쌍의 키와 그 키정보를 전송받는 PC로 이루어진 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 2】

제 1 항에 있어서, 상기 권한부여수단과 콘텐츠 공급수단은, 비밀 채널을 형성하기 위한 제 1 공유키를 생성하고, 상기 권한부여수단에서 콘텐츠 공급수단으로

공급되는 키 및 키정보는 상기 제 1 공유키에 의해 암호화된 후 콘텐츠 공급수단으로 전송되도록 하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 3】

제 1 항에 있어서, 상기 콘텐츠 공급수단은, 상기 권한부여수단과 동일하게 갖는 제 1 공유키를 이용하여 권한부여수단으로부터 전송된 키 및 키정보를 해독한 후 저장시키는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 4】

제 1 항에 있어서, 상기 콘텐츠 공급수단과 PC는 비밀 채널을 형성시키기 위해 제 2 공유키를 형성시키고, 콘텐츠 공급수단은 제 2 공유키를 이용하여 PC로 전송하는 키 및 키정보를 암호화하며, PC는 콘텐츠 공급수단과 공유한 제 2 공유키를 이용하여 키 및 키정보를 해독한 후 저장하는 것을 특징으로 하는 디지털 콘텐츠 복제 방지 시스템.

【청구항 5】

암호화 알고리즘에 의해 암호화된 디지털 콘텐츠를 전송받아 해독한 후 재생, 출력할 수 있는 디지털 콘텐츠 복제 방지 시스템에 있어서,

상기 암호화된 디지털 콘텐츠를 공급하거나, 또는 공급받아 재생, 출력할 수 있도록 제조키, 제조키 정보 및 상기 제조키와 제조키 정보를 갖는 제 1 테이블을 형성하고, 상기 테이블과 한쌍으로 휴대용 단말기의 ID, 제조키로 토큰을 암호화시킨 정보, 토큰을 갖는 제 2 테이블을 형성하고, 휴대용 단말기로 디지털 콘텐츠를 공급할 수 있도록 하는 한쌍의 자격 인증 키 및 자격 인증 키정보를 생성하여 송출

하는 권한부여수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 제조키 및 제조키 정보를 전송받는 휴대용 단말기 공급수단;

상기 권한부여수단으로 등록 요청신호를 송출하고, 등록 요청신호에 의해 발생된 암호화된 디지털 콘텐츠를 제공할 수 있는 자격이 부여되는 한쌍의 키와 그 키정보를 전송받고, 상기 권한부여수단의 제 2 테이블을 전송받는 콘텐츠 공급수단;

상기 콘텐츠 공급수단에서 공급하는 디지털 콘텐츠를 공급받아 재생, 출력시키고자 등록 요청신호를 콘텐츠 공급수단으로 송출하고, 상기 등록 요청신호에 의해 발생된 퍼블릭키와 퍼블릭키 정보를 전송받고, 제조키 정보를 콘텐츠 공급수단을 바이패스 시키며, 제 2 테이블로부터 상기 제조키 정보에 해당되는 테이블 정보를 검출하여 암호화한 후 전송하는 PC; 및

상기 권한부여수단에서 전송하는 제조키 및 제조키 정보를 입력받아 저장하고, PC를 통해 콘텐츠 공급수단으로 제조키 정보를 송출하며, 상기 PC에서 전송되는 자신에게 해당하는 암호화된 제 2 테이블의 제조키 정보를 입력받는 휴대용 단말기로 이루어진 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 6】

제 5 항에 있어서, 상기 휴대용 단말기에 장착되어 콘텐츠 공급부로부터 공급되는 디지털 콘텐츠를 휴대용 단말기를 통해 전송받아 저장하는 저장매체를 더 포함하는 것을 특징으로 하는 디지털 콘텐츠 복제 방지 시스템.

【청구항 7】

제 5 항에 있어서, 상기 권한부여수단과 콘텐츠 공급수단은, 시크리트 채널을 형성하기 위한 제 1 공유키를 생성하고, 상기 권한부여수단에서 콘텐츠 공급수단으로 공급되는 키 및 키정보는 상기 제 1 공유키에 의해 암호화된 후 콘텐츠 공급수단으로 전송되도록 하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 8】

제 5 항에 있어서, 상기 콘텐츠 공급수단은, 상기 권한부여수단과 동일하게 갖는 제 1 공유키를 이용하여 권한부여수단으로부터 전송된 키 및 키정보를 해독한 후 저장시키는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 9】

제 5 항에 있어서, 상기 콘텐츠 공급수단과 PC는 시크리트 채널을 형성시키기 위해 제 2 공유키를 형성시키고, 콘텐츠 공급수단은 제 2 공유키를 이용하여 PC로 전송하는 키 및 키정보를 암호화하며, PC는 콘텐츠 공급수단과 공유한 제 2 공유키를 이용하여 키 및 키정보를 해독한 후 저장하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 10】

제 5 항에 있어서, 상기 토큰은 권한부여수단에 의해 랜덤하게 발생하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 11】

제 7 항에 있어서, 상기 PC는 휴대용 단말기와 시크리트 채널을 형성시키기 위해 채널 키를 랜덤하게 발생시켜 암호화시킨 후 휴대용 단말기로 전송하고, 휴대용 단말기는 PC로부터 전송된 채널 키를 해독시켜 PC와 공유할 수 있도록 저장하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 12】

제 7 항 또는 제 11 항에 있어서, 상기 휴대용 단말기에서 암호화된 제 2 데이터블은, 휴대용 단말기에 저장된 제조키를 이용하여 해독시켜 토큰을 알아내고, 상기 토큰을 이용하여 PC와 공유하는 채널키를 해독시켜 저장하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 13】

PC에서 휴대용 단말기로 디지털 콘텐츠를 다운로드 받거나, 휴대용 단말기에서 PC로 디지털 콘텐츠를 업로드하는 디지털 콘텐츠 복제 방지 시스템에서,

상기 PC는, 디지털 콘텐츠가 무단 복제되는 것을 방지하기 위해 디지털 콘텐츠의 합법성을 체크하는데 필요한 정보를 갖는 데이터 베이스를 가지고, 상기 데이터 베이스는 PC에 의해 랜덤하게 발생되는 채널 키에 의해 암호화되거나, 암호화된 정보를 해독하여 데이터 베이스가 가지는 정보와 비교하여 디지털 콘텐츠의 무단복제여부를 판단하고,

상기 휴대용 단말기는, 상기 PC로부터 전송되는 암호화된 정보를 PC와 공유하는 채널 키를 이용하여 해독한 후 토큰을 업데이트하고, 업데이트된 토큰을 암호화한 후 상기 PC로 전송하는 것을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

시스템.

【청구항 14】

제 13 항에 있어서, 상기 데이터 베이스는, 디지털 콘텐츠의 타이틀 ID, 업
데이트 토큰 정보 영역, 디지털 콘텐츠의 현상태에 대한 정보 영역, 재생 제어 정
보 영역으로 나누어짐을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 15】

제 14 항에 있어서, 디지털 콘텐츠의 현상에 대한 정보 영역은, 복사, 전송
및 디지털 콘텐츠의 다운로드 또는 업로드 여부를 알 수 있도록 구성되어 있음을
특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항 16】

제 14 항에 있어서, 디지털 콘텐츠 재생 제어 정보 영역은, 재생회수에 대한
정보, 디지털 콘텐츠 재생 만료기간, 디지털 콘텐츠의 사면 기간에 대한 정보로 구
성되어 있음을 특징으로 하는 디지털 콘텐츠 무단 복제 방지 시스템.

【청구항17】

PLCM을 통해 디지털 콘텐츠 공급수단으로부터 공급되는 암호화된 디지털 콘텐츠를 입력받아 휴대용 저장매체로 전송해주는 휴대용 단말기를 갖는 복제 방지 시스템에 있어서, (LCM에서 직접 휴대용 저장매체로 저장할 수도 있음)

블록섹터의 물리적 주소, 랜덤한 수 및 PLCM에서 생성하여 전송되는 시크릿 키를 입력으로 받아 함수처리하고, 함수 처리된 결과값으로 디지털 콘텐츠의 헤더를 암호화하여 송출하는 휴대용 단말기; 및

상기 휴대용 단말기로 블록섹터의 물리적 주소를 읽어들이고, 전송하고, 휴대용 단말기에서 랜덤하게 발생하는 수를 키 값으로 저장하며, 휴대용 단말기를 통해 입력되는 암호화된 디지털 콘텐츠 및 함수 결과값에 의해 다시 암호화된 헤더 정보를 섹터 데이터로 저장하는 휴대용 저장매체로 이루어짐을 특징으로 하는 무단 복제를 방지하기 위한 휴대용 저장매체를 갖는 시스템.

COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

ABSTRACT

【요약】

사용자가 재생하고자 다운받은 암호화된 디지털 콘텐츠가 무단 복제되는 것을 방지하기 위해 사용자와 연결되는 모든 시스템이 서로 상호간에 공유할 수 있는 다수의 키를 생성하여 공유하고, 상호간에 형성된 시크리트 채널을 이용하여 디지털 콘텐츠를 다운로드 또는 업로드하는 디지털 콘텐츠 무단 복제 방지 시스템이 개시되어 있다.

디지털 콘텐츠를 공급하는 수단이 권한부여수단으로부터 합법적으로 디지털 콘텐츠를 공급할 수 있다는 권한을 부여받는다. 그리고 PC는 상기 디지털 콘텐츠 공급수단으로부터 인증을 받으며, 이때 디지털 콘텐츠 공급수단과 PC는 공유키를 형성하여 둘 사이에 시크리트 채널을 형성한다. 그리고, 휴대용 단말기는 PC를 통해 디지털 콘텐츠 공급수단으로부터 인증을 받으며, PC와 휴대용 단말기는 채널 키에 시크리트 채널을 형성한다. 그리고 PC와 휴대용 단말기에 사이에 디지털 콘텐츠를 각각이 가지고 있는 제어 상태에 따라 다운로드 또는 업로드되도록 한다. 따라서, 디지털 콘텐츠 공급수단, PC 및 휴대용 단말기 사이에서 전송되는 디지털 콘텐츠의 무단으로 복제하는 불법 복제를 방지할 수 있다는 효과가 있다.

[illegible]

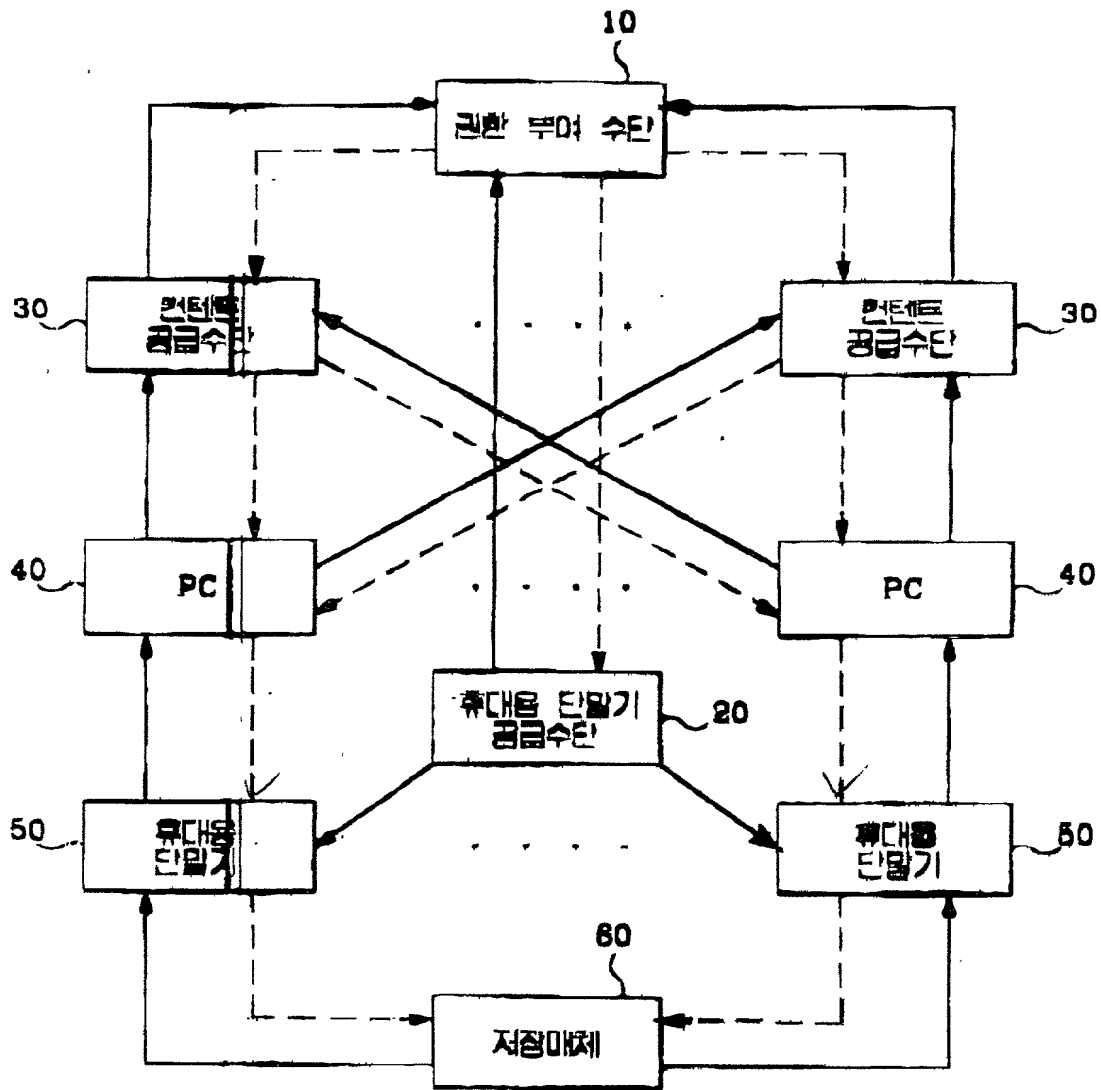


FIG. 1

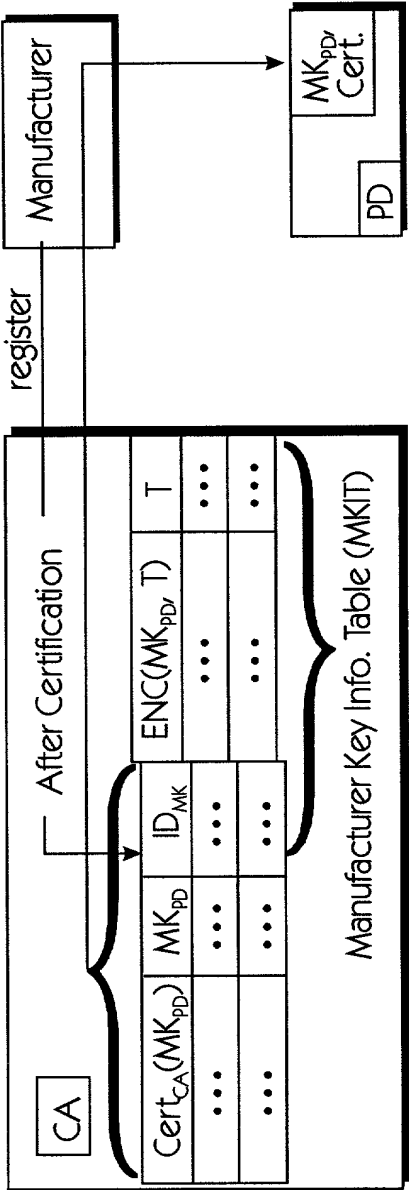


FIG. 2

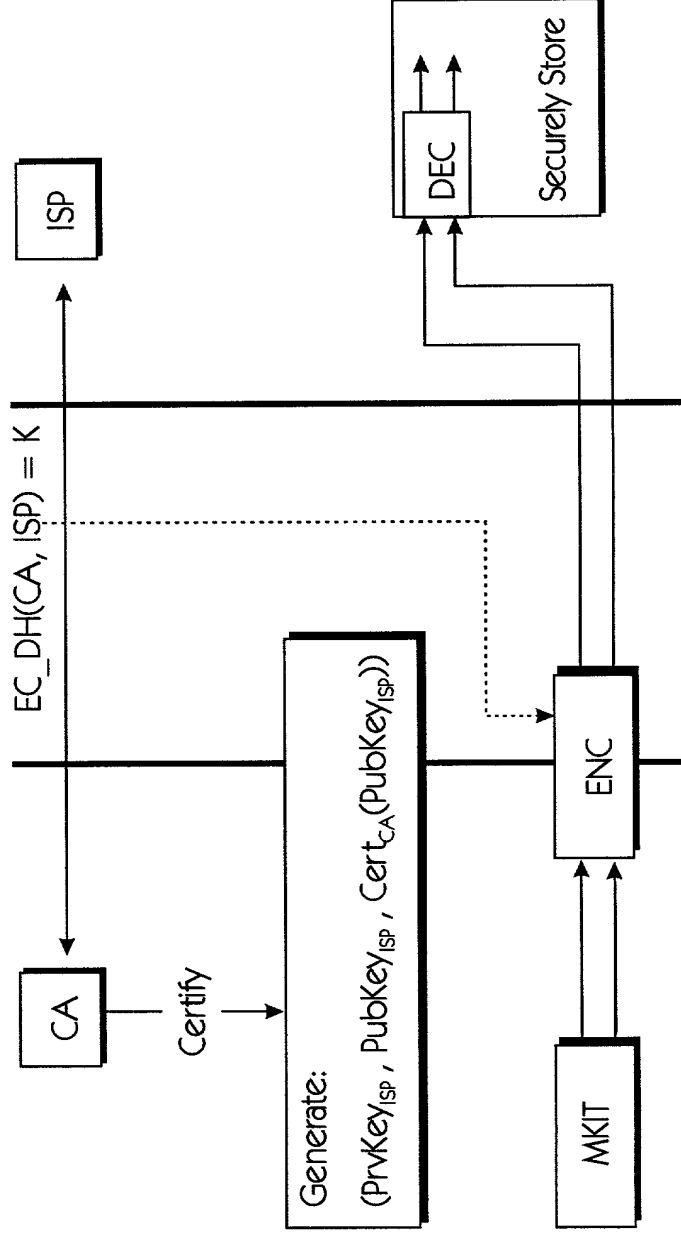


FIG. 3

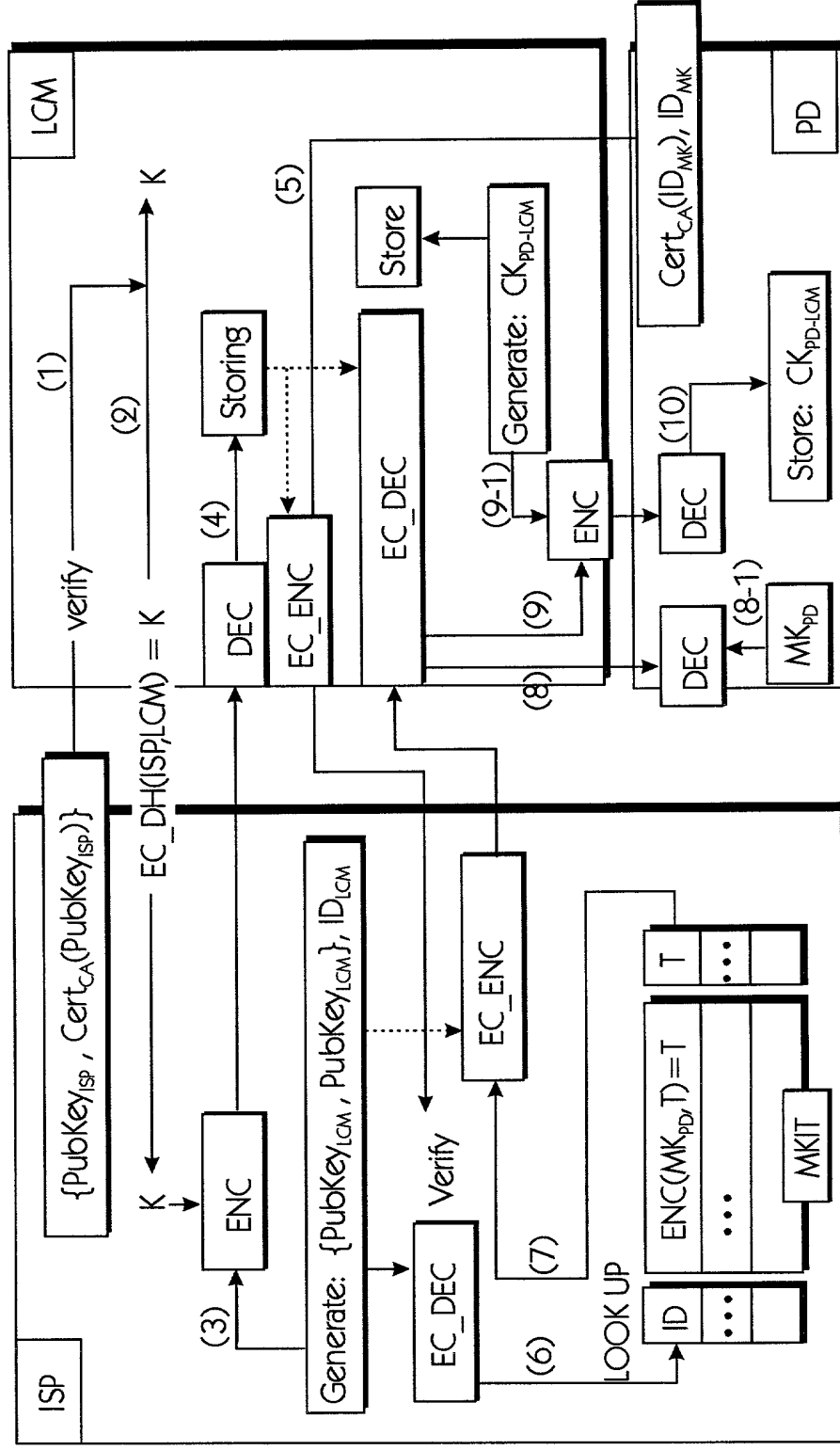


FIG. 4

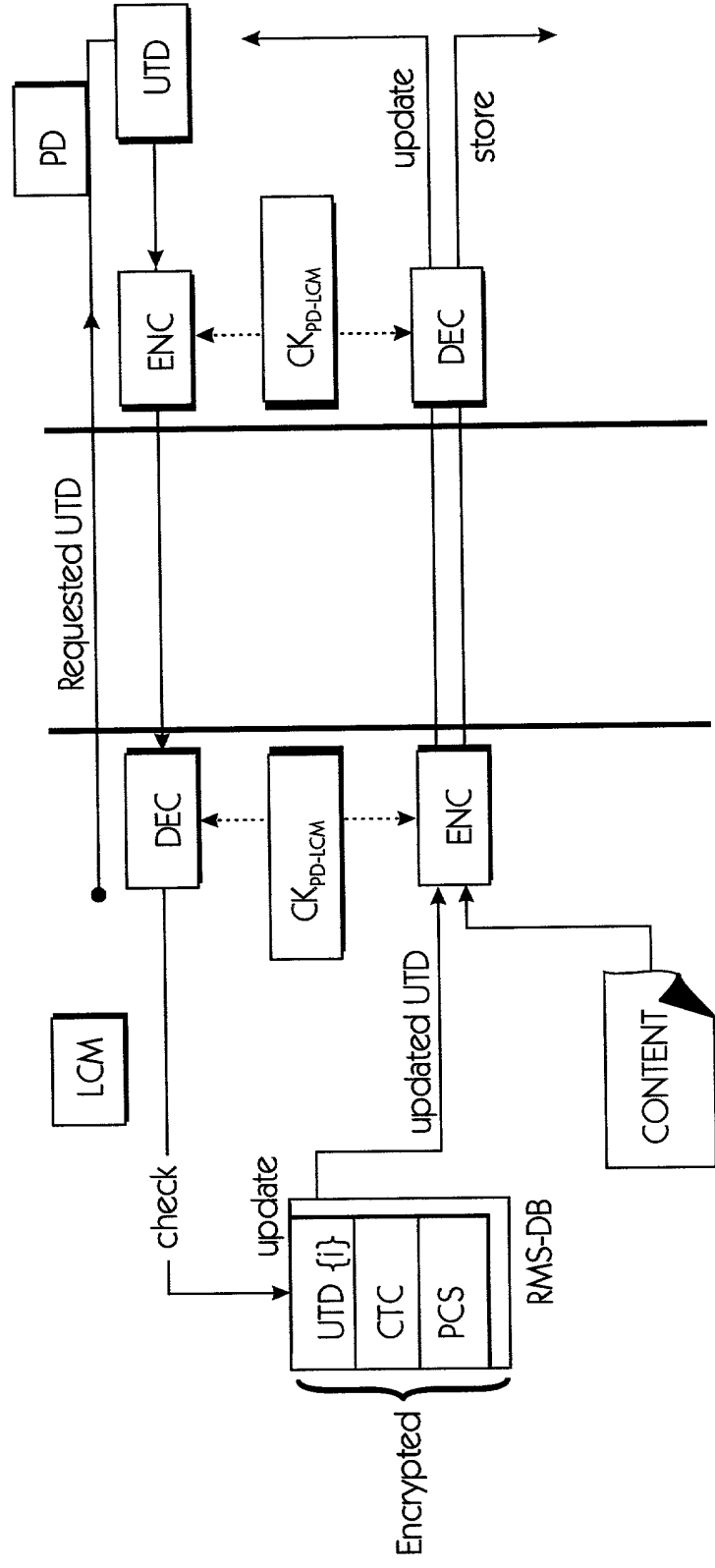


FIG. 5

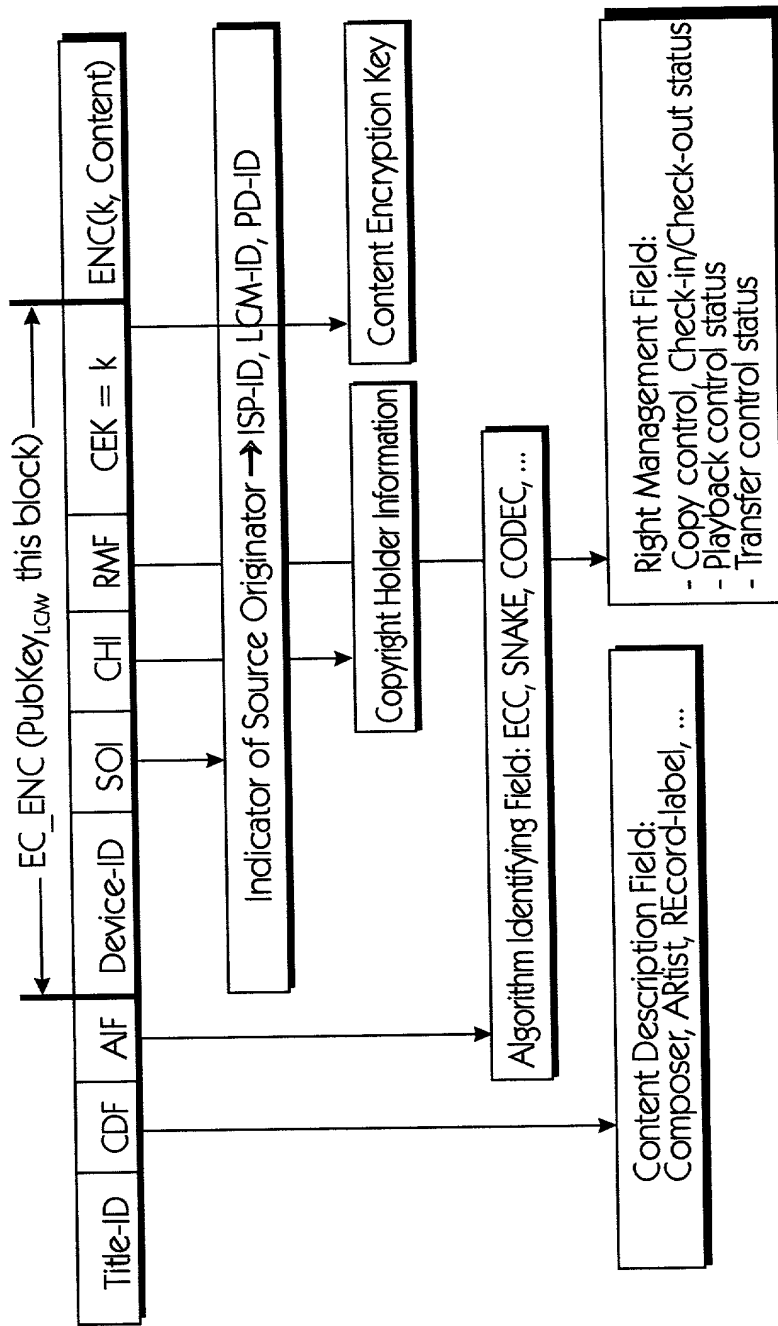


FIG. 6

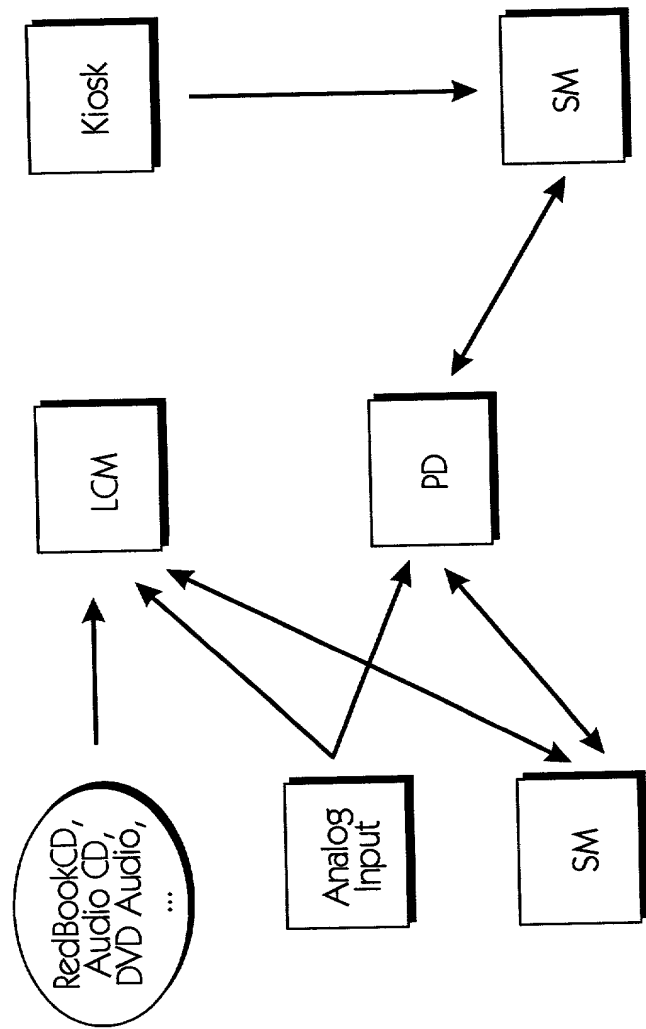


FIG. 7

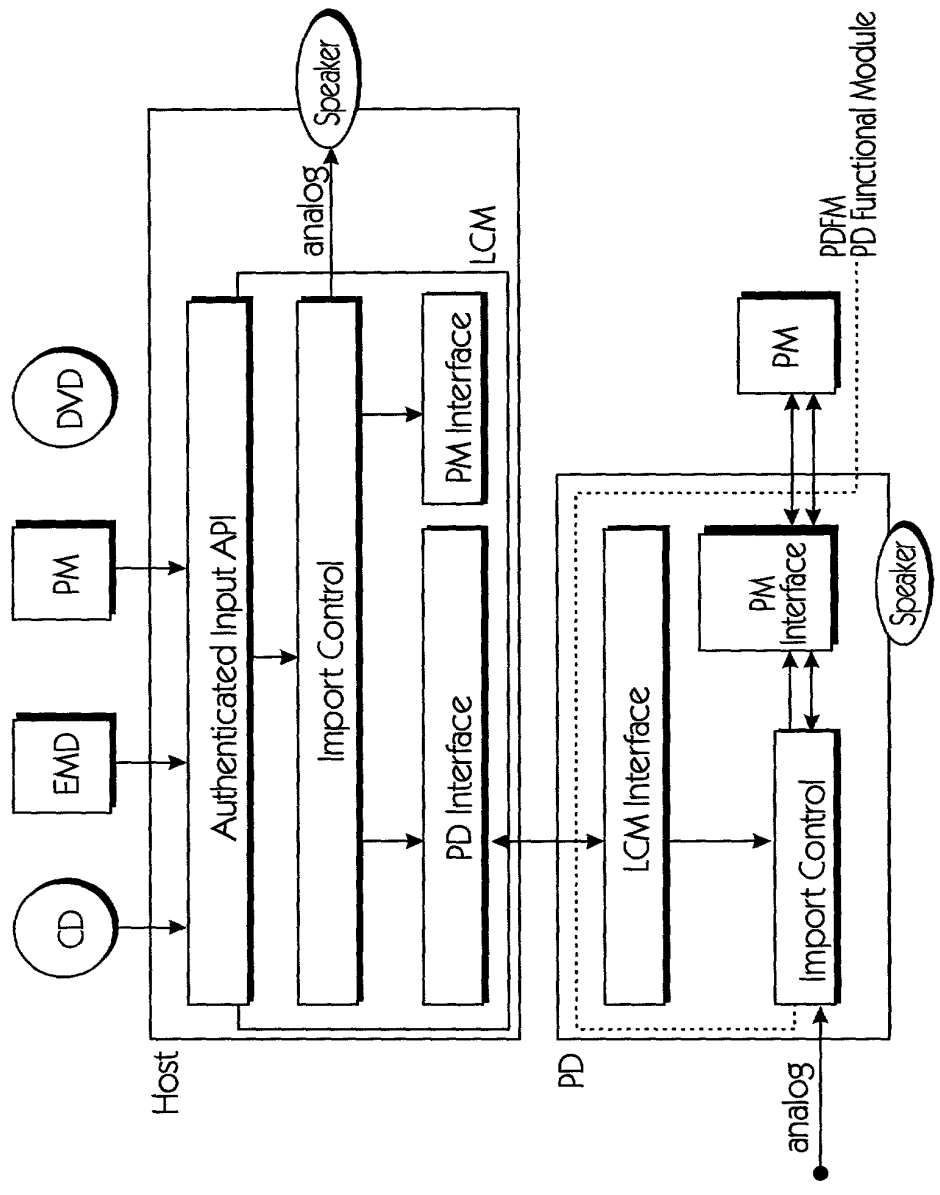


FIG. 8

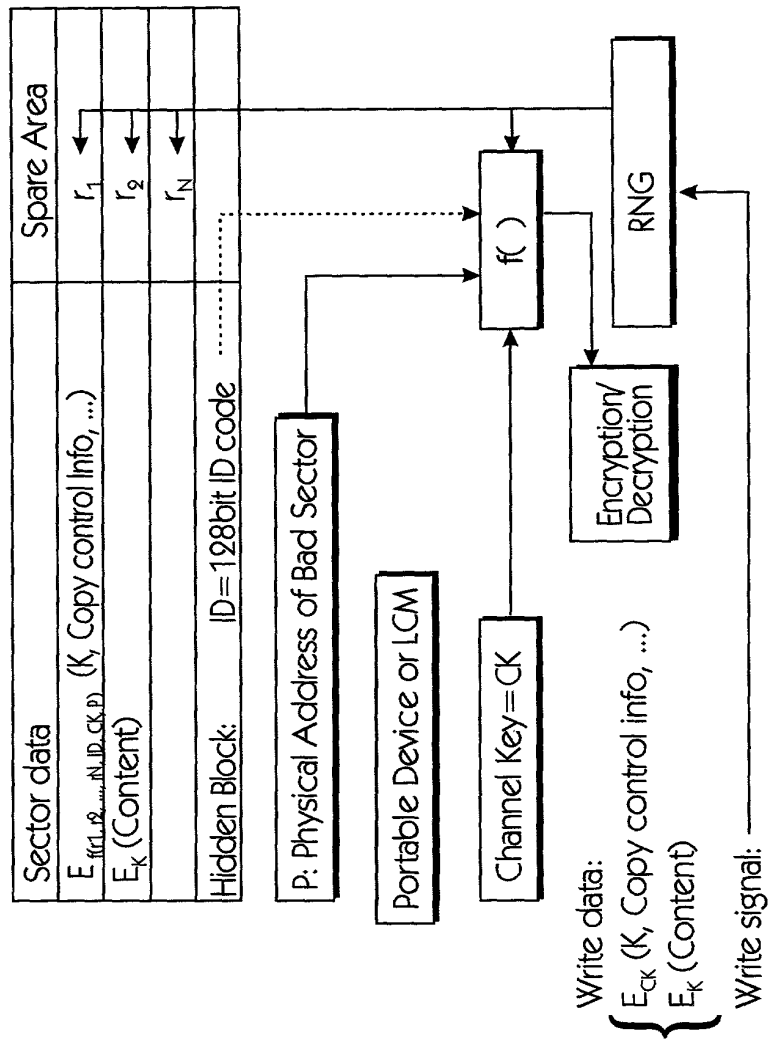


FIG. 9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

CHANG-HYI LEE *et al.*

Serial No.: *to be assigned*

Examiner: *to be assigned*

Filed: 30 April 1999

Art Unit: *to be assigned*

For: COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

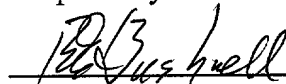
TRANSMITTAL OF DECLARATION

Assistant Commissioner
for Patents
Washington, D.C. 20231

Sir:

This transmittal accompanies a Declaration without the signature by the inventor(s), for the above-captioned application. A Substitute Declaration with the inventor(s)'s signature will be filed upon receipt of the Serial No. for the above-captioned application.

Respectfully submitted,


Robert E. Bushnell,
Attorney for the Applicant
Registration No.: 27,774

Suite 300, 1522 "K" Street, N.W.
Washington, D.C. 20005
(202) 638-5740

Folio: P55690
Date: 04/30/99
I.D.: REB/kf

DECLARATION

AS A BELOW NAMED INVENTOR, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe that I am the original, first and sole (if only one name is listed below), or an original, first and joint inventor (if plural names are listed below), of the subject matter which is claimed and for which a patent is sought on the invention entitled:

TITLE: COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

the specification of which either is attached hereto or otherwise accompanies this Declaration, or:

☐ was filed in the U.S. Patent & Trademark Office on _____ and assigned Serial No. _____,

☐ and (if applicable) was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability and to the examination of this application in accordance with Title 37 of the Code of Federal Regulations §1.56. I hereby claim foreign priority benefits under Title 35, U.S. Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, or §119(e) of any United States provisional application(s), listed below and have also identified below any foreign applications for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Priority Claimed:

Yes [X] No []

39808/1998 Republic of Korea 24 September 1998
(Application Number) (Country) (Day/Month/Year filed)

39809/1998 Republic of Korea 24 September 1998
(Application Number) (Country) (Day/Month/Year filed)

Yes [X] No []

I hereby claim the benefit under Title 35, U.S. Code, §120, of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application(s) in the manner provided by the first paragraph of Title 35, U.S. Code, §112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, The Code of Federal Regulations, §1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.) (Filing Date) (STATUS: patented, pending, abandoned)

(Application Serial No.) (Filing Date) (STATUS: patented, pending, abandoned)

I hereby revoke all previously granted powers of attorney and appoint the following attorneys: Robert E. Bushnell, Reg. No. 27,774, Michael D. Parker, Reg. No. 34,973, and Henry M. Zykorie, Reg. No. 27,477, to prosecute this application and to transact all business in the U.S. Patent & Trademark Office connected therewith and with any divisional, continuation, continuation-in-part, reissue or re-examination application, with full power of appointment and with full power to substitute an associate attorney or agent, and to receive all patents which may issue thereon, and request that all correspondence be addressed to:

Robert E. Bushnell,
Attorney-at-Law
Suite 300, 1522 "K" Street, N.W.
Washington, D.C. 20005-1202

Payor No. 008439
Area Code: 202-638-5740

I HEREBY DECLARE that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 U.S. Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST OR SOLE INVENTOR: CHANG-HYI LEE

Citizenship: Republic of Korea

Inventor's signature: _____
Residence & Post Office Address: #416, Maetan-dong, Paldal-gu, Suwon-city, Kyungki-do, Republic of KOREA

Date: _____

FULL NAME OF SECOND JOINT INVENTOR: HO-SUK CHUNG

Citizenship: Republic of Korea

Inventor's signature: _____
Residence & Post Office Address: #416, Maetan-dong, Paldal-gu, Suwon-city, Kyungki-do, Republic of KOREA

Date: _____

FULL NAME OF THIRD JOINT INVENTOR: EN-SEONG KANG

Citizenship: Republic of Korea

Inventor's signature: _____
Residence & Post Office Address: #416, Maetan-dong, Paldal-gu, Suwon-city, Kyungki-do, Republic of KOREA

Date: _____

FULL NAME OF FOURTH JOINT INVENTOR: _____

Citizenship: _____

Inventor's signature: _____
Residence & Post Office Address: _____

Date: _____

☐ Additional inventors are being named on separately numbered sheets attached hereto.